Microsoft® Windows® 2000 and Microsoft® Exchange 2000 Server Deploying the Active Directory Connector

PT101
Version 1.1

From the Exchange 2000 Server Pre-emPt Series

Paul Bowden
Program Manager - Europe
Microsoft Exchange Server Product Unit

PLATINUM

Microsoft Technical Readiness
Service Partner Support Sales

© 1999 Microsoft Corporation. All rights reserved.

The information contained in this White Paper represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

The BackOffice logo, Microsoft, Outlook, Win32, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

Contents

MICROSOFT® WINDOWS® 2000 AND MICROSOFT® EXCHANGE 2000 SERVER DEPLOYING THE ACTIVE DIRECTORY CONNECTOR....1

CONTENTS....III

ACKNOWLEDGMENTS....VI

DOCUMENT VISION AND SCOPE....1

INTRODUCTION....2

What Is the ADC?....2
Versions of the ADC....2
Exchange 2000 and the Active Directory....2
What Does the ADC Consist Of?....3
Connection Agreements....3
Configuration Connection Agreements and Site Replication Service....3

DEPLOYMENT PLANNING....5

Requirements....5
Drivers for Deploying the ADC....5
Questions You Need to Ask....5

TECHNICAL PLANNING....8

Primary Windows NT Account for Exchange Mailboxes....8
Exchange Server Versions....8
Schema Updates....8
Installing Exchange Server 5.5 on a Windows 2000 Server....8
Where Should the ADC Be Installed?....9
Deploying Multiple ADC Servers....10
LDAP Ports and Protocols....10
Scenario: Two Active Directory Domains, Three Exchange Sites....11
Container Mapping....11
Scenario #1: Simple Mapping....12
Scenario #2: Split Containers....12

RESOURCE USAGE....17

Server Resources Consumed by the ADC....17
Network Consumption....17
Using the Site Replication Service with Exchange 2000 Server....18
Downstream Replication Traffic....18

HOW THE ADC WORKS....19

Initial Replication....19
Detecting Changes in the Exchange Directory....19
Detecting Changes in the Active Directory....19
Object Class Mapping and Attributes....19
Duplicate Object Detection....20
Schema Discovery....20

IMPLEMENTATION WALKTHROUGH....21

ADC Installation....21
Configuring Attribute Replication and Object Matching....21
Creating a Connection Agreement....23

POST INSTALLATION....31

Replicated Objects in the Active Directory....31

Replicated Objects in the Exchange Directory....31
Attributes of the Connection Agreement....32

TROUBLESHOOTING....33

Event Logs....33
Time Synchronization....33
Directory Inconsistencies....33

ADVANCED CONFIGURATION....35

Do I Need Anything Else?....35
Tools....35
Changing the LDAP Search Filter Rule....35
Changing the Attribute Map....36

Appendix: Schema Updates Made by the Exchange 2000 Server ADC....37

Acknowledgments

Many thanks to the following people for their time and enthusiasm. No white paper is produced without many people going out of their way to assist.

Exchange Product Group

Peter Waxman

Neil Koorland

John Freeman

Neil Shipp

David Madison

Windows 2000 Product Group

Steven Judd

Behrooz Chitsaz

Product Support Services (PSS)

Paul Appleby

Andy Moss

Brent Albrecht

Microsoft Consulting Services

Peter Nilsson

Darren Strange

Dave Trulli

Others

Laura Payne (Exchange Program Manager, Service Readiness)

Everyone on PlatChat

Philip Beville, Richard Minty, and the rest of the Exchange Global Engineering team at Credit Suisse First Boston

Document Vision and Scope

The purpose of this document is to provide you with an understanding of how to deploy the Active Directory Connector (ADC).

After reading this document, you should understand:

- What the ADC is.
- What to consider before implementing the ADC.
- How the ADC works.
- How to deploy the ADC.

This paper provides a walkthrough of an implementation with screenshots. This will help to solidify your understanding of the steps necessary to configure this component.

Although the ADC can be used to synchronize many different types of directories with Active Directory, this paper covers only synchronization to the Exchange Server 5.5 Directory Service and migration to Exchange 2000 Server.

This information should be part of the learning cycle for Exchange 2000. To gain a full understanding of the other technologies the product includes, read the other documents in this series:

- PT100 – Windows 2000 and Exchange 2000 Server Terminology Primer
- PT102 – Exchange 2000 Server Directory Access and Integration with Windows 2000
- PT103 – Exchange 2000 Server Coexistence and Upgrades
- PT104 – Understanding Message Routing in Exchange 2000 Server
- PT105 – Understanding Exchange 2000 Server Storage Technology
- PT106 – Deploying Exchange 2000 Server Real-time Collaboration Services
- PT107 – Collaboration with Exchange 2000 Server

Note The information in this document is based on Microsoft® Windows® 2000 Release Candidate 2 and Microsoft® Exchange 2000 Server Beta 3.

Introduction

What Is the ADC?

The Active Directory Connector (ADC), is the component that synchronizes the Windows 2000 Active Directory with the Microsoft® Exchange Server 5.5 directory. This synchronization can be used to aid in the implementation of the Active Directory for organizations that have already deployed Exchange Server 5.5 and is a necessary stage for achieving coexistence between Exchange Server 5.5 and Exchange 2000 Server.

In the future, ADC technology may be extended to support synchronization of other directories, such as Netscape Directory Server, DCL X.500, generic Lightweight Directory Access Protocol (LDAP) directories, and other Windows 2000 Active Directories.

The ADC works in the following ways:

- Uses the LDAP application programming interface (API) to perform fast replication between the two directories.
- Hosts all active replication components on the Active Directory, not the foreign system.
- Replicates only changes between the two directories whenever possible.
- Maintains object fidelity through replication (for example, the Active Directory **Group** object maps to the Exchange **Distribution List** object).
- Hosts multiple connections on a single Active Directory Server and manages these through Connection Agreements (CAs).

Versions of the ADC

The basic replication functionality of the ADC is included with Windows 2000; however, when you install Exchange 2000, an update is installed.

Windows 2000 ADC

Included with Windows 2000, the Windows 2000 ADC replicates rich directory information in Exchange 5.5 to the Active Directory and vice versa. Many customers have already invested heavily in the Exchange directory, and much of this data can be uploaded in bulk to the Active Directory, which decreases implementation time. Through synchronization, the Active Directory administrator can also perform basic management functions for Exchange 5.5 users.

Exchange 2000 Server ADC Update

The Exchange 2000 Server ADC update is an enhanced connector included with Exchange 2000 Server. Whereas the Windows 2000 ADC simply replicates objects in the Exchange site-naming context (for example, **Recipients** containers) to the Active Directory, the Exchange 2000 ADC also replicates data from the configuration-naming context, thus providing support for mixed-vintage Exchange sites and downstream routing.

The upgrade path between the two versions of the ADC is seamless. Customers can deploy the Windows 2000 ADC to build their basic Active Directory very quickly, and when ready, they can install the updated ADC when installing the first Exchange 2000 server.

Exchange 2000 and the Active Directory

Exchange 2000 no longer includes a directory service of its own; instead, it uses the Active Directory provided by Windows 2000 for object browsing, security, and name resolution. For companies that have already deployed Exchange Server 5.5, coexistence between the Exchange 5.5 directory and the new Active Directory is a vital prerequisite for the Exchange 2000 upgrade process.

However, once Exchange 2000 is deployed, the Active Directory becomes the Global Address List for those Microsoft® Outlook® messaging and collaboration client users who have their mailboxes on Exchange 2000, so it is important for both directories to have complete information about each other.

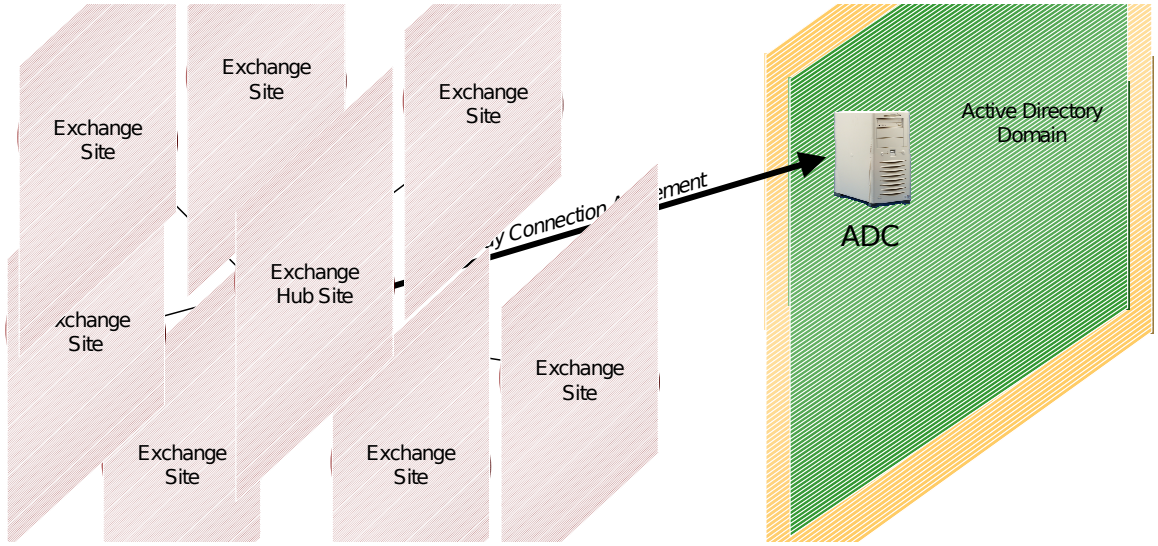
What Does the ADC Consist Of?

The ADC is installed as an additional component on top of Windows 2000 and Exchange 2000. On installation, you will notice a new Windows service called the MSADC. This service can be started and stopped just like any other service. Also installed are a snap-in and an .msc file for configuring the CAs between the Active Directory and the Exchange target directory.

Connection Agreements

Installing the ADC on a server simply defines a service within Windows 2000. To establish a relationship between an existing Exchange site and the Active Directory, you must configure a CA. The CA holds information, such as the server names to contact for replication, object classes to replicate, target containers, and the replication schedule. It is possible to define multiple CAs on a single ADC; each of which can go from the Active Directory to a single Exchange site or to multiple Exchange sites. For performance reasons, it is recommended that each ADC server manage no more than 50 to 75 individual CAs, depending on the specification of the computer. In enterprise environments, you may want to deploy multiple ADC servers to improve performance.

If you are uploading existing Exchange directory data to the Active Directory, you can create a single CA between the Active Directory and one Exchange site. Because all site information from the entire Exchange organization can be gained from any Exchange 5.5 server in the organization, all of the objects and sites can be pulled through a single connection. The connection would be defined as a *one way from Exchange* agreement, allowing the Active Directory data to be updated when the Exchange directory is modified.



In another scenario, in which an Exchange 2000 server coexists in the same site with previous versions of Exchange Server and you want central directory management from the Active Directory, you can create a *two way* CA. This type of connection allows both reads from and writes to both directories, and as such, can only communicate with one Exchange site. However, you can create multiple CAs (on the same ADC server if desired) if multiple Exchange sites exist in the Exchange 5.5 directory.

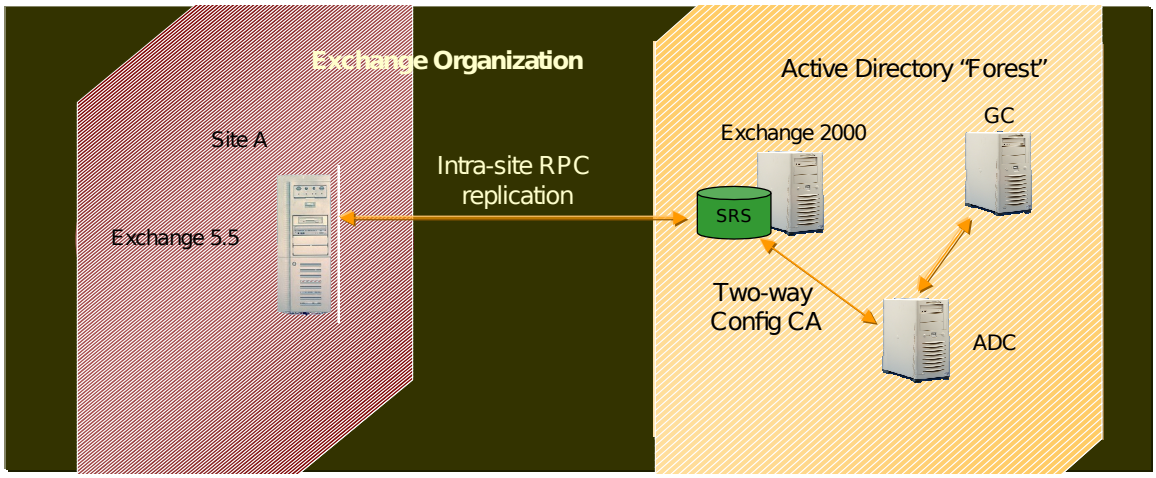
Configuration Connection Agreements and Site Replication Service

A standard CA replicates recipient objects and information between the two directories; however, when an Exchange 2000 server belongs to an existing Exchange 5.5 site, configuration information must be replicated. This allows the Exchange 2000 server to be represented in the Exchange site server list so that earlier versions of Exchange can send and receive messages as seamlessly as if the new server were running Exchange 5.5. Additionally, doorway or route information must be replicated between the two directories to allow Exchange 2000 servers to send messages to specialized connectors that exist on the Exchange 5.5 servers and vice versa. All configuration information is replicated through a unique instance of a CA ,which is known as a Configuration Connection Agreement or ConfigCA.

Unlike standard Connection Agreements, ConfigCAs are configured automatically by Exchange Server rather than having to instantiate them manually. Additionally, the agreement for replicating configuration-naming context data is between the Active Directory and the Exchange Site Replication Service (SRS) rather than between the Active Directory and Exchange 5.5 server. The SRS is a component installed by Exchange 2000 Server and is similar to the Exchange 5.5 Directory Service, although the Messaging Application Programming Interface (MAPI) is disabled. When an Exchange 2000 server is installed into an Exchange 5.*x* site, the SRS is used for intra-site directory replication over Remote Procedure Calls (RPC). If an Exchange 5.5 directory-replication bridgehead server is upgraded to Exchange 2000, the SRS provides mail-based directory replication to downstream Exchange 5.*x* sites.

The first ConfigCA created by the SRS is named **Master_Config CA_*ORGNAME*** and although the name can be seen in the Active Directory Connector management snap-in, the agreement is read-only, and thus cannot be modified. Like a standard Exchange directory service, the SRS supports direct LDAP calls and listens on port 379 to avoid port contention with other LDAP services running on the computer. For more information about how the Site Replication Service works, see “PT103 – Exchange 2000 Server Coexistence and Upgrades.”

After replication, all Exchange 5.*x* sites are represented in the Active Directory as administrative groups, and conversely, Exchange 2000 servers in the administration group are represented in the Exchange 5.*x* site.



Deployment Planning

Requirements

Before you deploy the ADC and its Connection Agreements (CAs), it is vitally important that you consider all of the organization's business requirements to avoid problems later on. The ADC can be configured to make fundamental changes to directories (including deleting objects); therefore, incorrect deployment could result in destabilization of the existing Exchange infrastructure.

Drivers for Deploying the ADC

There are four main reasons why companies deploy the ADC:

- To leverage the rich information about users in the Exchange directory by replicating it (rather than rekeying it) to the Active Directory (this replicating may either be for Active Directory testing purposes or for the production environment).
- To replicate existing Exchange 5.5 directory data to Active Directory so that new third-party applications can take advantage of it.
- To create an environment in which both Active Directory and the Exchange directory can be managed from one management application.
- To enable Exchange 2000 Server to be deployed while coexisting with the installed Exchange environment.

If none of these reasons apply to your organization, you should reconsider deploying the ADC. For example, Exchange Server 5.5 can run efficiently without the ADC, even when the domains and servers have been upgraded to Microsoft Windows 2000 and Active Directory. The Windows 2000 Active Directory continues to provide authentication services for Exchange just as Windows NT 4.0 did, and Microsoft® Outlook® continues to use the directory service in Exchange.

Questions You Need to Ask

Assuming that you need to deploy the ADC, here are the questions you need to ask. These discussion points should involve the business sponsor, Active Directory planning team, Exchange 2000 planning team, and existing support and administration staff. The answers to these questions will dictate how you should deploy the ADC.

Do we want to manage all objects from the Active Directory?

Using the ADC, you can use a single tool for administration of both the Active Directory and the Exchange directory; however, functionality always comes at a price. If using a single tool for administration is a requirement, you need to deploy a CA to each of your existing sites, which requires Lightweight Directory Access Protocol (LDAP) and Remote Procedure Calls (RPC) connectivity, and you need to configure them so that they can write to the Exchange directory. Because the ADC replicates objects from the Exchange directory to the Active Directory, it must write various attributes to each Exchange object it comes in contact with. As the object is modified, there is a one-time hit because each Exchange object in the site is replicated a second time within the native environment. In very large Exchange systems this can potentially cause directory and network flooding. To mitigate this risk, you should stagger the deployment of CAs.

If you use the Exchange Administrator program to manage the Exchange 5.5 environment, the majority, if not all, of the CAs can be defined as one-way from Exchange (that is, read-only from the Exchange Server). Additionally, you can deploy a single one-way agreement to only one Exchange site and pull all of the required information from that point instead of defining an agreement to each site. This will further reduce the management and replication overhead of the ADC.

How many Active Directory domains are we planning?

Unlike previous versions of Exchange, the Active Directory does not tie the namespace to the directory replication model; for example, when deploying Exchange Server 5.5, the

business may have a requirement to seamlessly move users between Exchange servers. To meet this requirement, some customers deploy very wide Exchange sites that span low-bandwidth networks. Because the Exchange site requires that the directory replication (and messaging) model be meshed RPC, additional management and administration challenges are produced.

Although the Active Directory is far more flexible in terms of namespace and the replication model, the initial release of Windows 2000 requires that *domain naming context* replication transfers between domain controllers occur over synchronous RPC. In some environments, this may result in the deployment of many small domains. As the number of domains in the Active Directory increases, the number of CAs also increases.

One of the other considerations for deployment of the ADC is the number of ADC servers required to replicate the data. Although an ADC can have CAs for multiple Active Directory domains, the protocol used between the ADC server and Exchange 5.5 directory is mainly LDAP and a few RPC requests (the latter is used when writing to the Exchange directory), and both require direct Internet Protocol (IP) connectivity. If a global organization has offices and Exchange sites in many countries, it is unlikely that the company will deploy only one ADC server. Most companies install an ADC server in each major geographical region.

Will we upgrade our Master/Account domains before deploying the ADC?

Each Exchange mailbox is mapped to a primary Windows NT account, which is normally mapped to a master-accounts domain. Ideally, each of these account domains should be upgraded to Windows 2000 and the Active Directory before the ADC is deployed. This is actually not necessary, however, because only the primary domain controller of these domains requires the upgrade; all other backup domain controllers and member servers can reside in the *mixed-mode* domain.

So how does this make a difference to the ADC? Once you start to install Exchange 2000 servers in the Active Directory, Outlook is able to detect only directory objects that are represented in the Active Directory, so you may need to configure additional CAs as part of the Exchange 2000 deployment process. You need to ensure that all existing Exchange objects, including those mapped to Windows NT 4.0 domains, are represented in the Active Directory.

For example, let’s say one of your existing Exchange sites has **Mailbox** objects that have their primary Windows NT account mapped to a pure Windows NT 4.0 domain. If you define a CA for those **Mailbox** objects, you must decide how those objects are to be created within the Active Directory. Because **Mailbox** objects cannot be mapped to a security object within the Active Directory (they only exist in the Windows NT 4.0 domain), by default, a **disabled Windows User** object is created.

Note In versions of the ADC shipped with Windows 2000 Beta 3 and later, you can prevent the ADC from creating an object altogether if a mapping cannot be performed between the Exchange directory object and the Windows 2000 Active Directory; however, if an Exchange 2000 server exists in the environment, you need to have all user objects present in the Active Directory to allow Exchange 2000 users to address messages to users on earlier versions of Exchange Server.

If you decide to create either **Enabled Windows User** or **Disabled Windows User** objects in the Active Directory, you must run the Active Directory Cleanup Wizard (Adclean.exe) when the Windows NT4.0 domain is eventually upgraded. The wizard will merge the two security principals into one object, retaining the security identifier of the deleted object in the **SIDHistory** attribute of the remaining object.

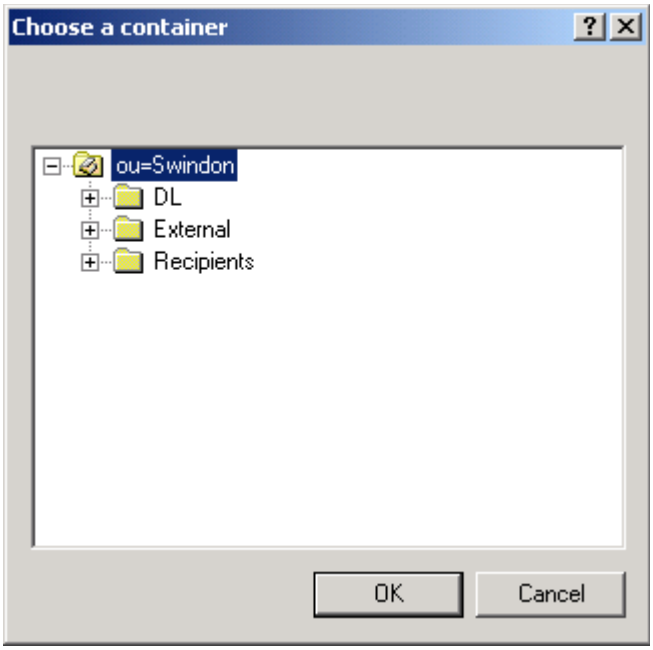
How have we defined our container structure in the existing Exchange system?

By default, an Exchange site has only the **Recipients** container defined. Some companies have created other containers for different types of objects. It is relatively

uncommon for companies to create containers for each business unit or department because it is extremely difficult to move objects between containers. It is quite common, though, for companies to create special containers to hold different object classes, such as **Distribution Lists** and **Custom Recipients**. Depending on the existing structure in the Exchange directory and the proposed structure in the Active Directory, you may need to decide on a strategy for replicating those objects to equivalent containers.

For example, let's say that an Exchange site has three containers: **Recipients**, **Distribution Lists**, and **External Addresses**.

- To retain the same structure in the Active Directory, create a single CA. The source container in the Exchange directory is the *site* because the subcontainers can be automatically created in the Active Directory and populated.



- To consolidate all three Exchange containers into a single container or organizational unit in the Active Directory, create a single CA and individually choose each of the three containers as the source.
- To have complete control over each container, specifying target container or organizational unit replication times and deletion variables, create three separate CAs.
- To change the model completely so that the Active Directory structure represents the business model, configure a single CA, choose the containers individually, or choose the site level, and then replicate them to a dummy target container or organizational unit in the Active Directory. Once the objects have been replicated, you can use the Active Directory Users and Computers snap-in to move those objects (by right-clicking the object) to the correct container or organizational unit. The ADC retains the relationship between the two objects even though they have been moved. It can do this because of the match between the object and the globally unique identifier (GUID). If you use this approach, remember to include the new container or organizational unit as a source container for a two-way CA; otherwise, changes made to the object in the Active Directory are not replicated back to the Exchange directory.

Primary Windows NT Account for Exchange Mailboxes

The object class fidelity that you get between the legacy Exchange directory and Active Directory mainly depends on the deployment of the Active Directory and a Microsoft Windows 2000 domain within the Microsoft Exchange 5.5 environment. For total fidelity, you should plan on upgrading at least one domain controller to Windows 2000 in the domain in which the primary Windows NT account exists for Exchange mailboxes. In essence, if all Exchange 5.*x* mailboxes have their primary Windows NT account mapped to a Windows 2000 domain, full clarity of object classes, attributes, and two-way replication can be established. If the ADC is deployed between the Active Directory and an Exchange system mapped to Windows NT 4.0 domains, you need to decide how to map the object classes (**Contact**, **User**, **disabled Windows User**). By default, an Exchange 5.5 **Mailbox** object with a Windows NT 4.0 domain mapping is replicated to the Active Directory as a **disabled Windows User** object. Your decision of which object class to create depends on the expected lifetime of the resulting object; for example, if you want the object present only in the Active Directory so that **Mailbox** objects on Exchange 2000 servers can mail to these recipients, you can use the **mail-enabled Contact** object class. However, if you are not planning to upgrade the existing domain structure in the conventional manner but want to implement a new Active Directory environment, configuring the ADC to create **User** objects will simplify your overall project.

Exchange Server Versions

When you define a Connection Agreement (CA) to an Exchange site, the target directory bridgehead must be Exchange Server 5.5 SP2 (or later), even if you are defining a one-way CA. This is because although Exchange 5.0 supports read Lightweight Directory Access Protocol (LDAP), it doesn't support the additional LDAP paging support required to optimize the throughputof the ADC.

Other Exchange servers within the site are not required to run Exchange Server 5.5.

Schema Updates

When the Exchange 2000 ADC is configured with a two-way CA in the Exchange 5.5 site, the schema version is checked and updated as required. If you upgrade one of the servers in the site to Exchange 5.5 SP3, the schema is up-to-date; if not, the directory service on the target Exchange bridgehead is stopped, the new schema updates are added, and the service is started again. The actual schema changes are listed in the appendix of this document.

Installing Exchange Server 5.5 on a Windows 2000 Server

Many customers may want to deploy Exchange 5.5 Server on Windows 2000 before Exchange 2000 is available. This is possible, but Exchange 5.5 SP3 should be installed to fully support this configuration. After the Exchange Server installation, you may notice that the Active Directory contains no information about Exchange. Also, when you try to create new **User** objects in the Active Directory Users and Computers snap-in, you are not prompted to create a **Mailbox** object. On Windows NT 4.0, Setup for Exchange Server installs the Mailumx.dll library to support User Manager for Domains. With this, the Exchange Administrator and User Manager programs appear to be linked together. Because Windows 2000 uses a different administration architecture, this linking is no longer possible through the installed DLL.

If you use the Exchange Administrator program to automatically create Active Directory **User** objects, only a small set of fields are populated:

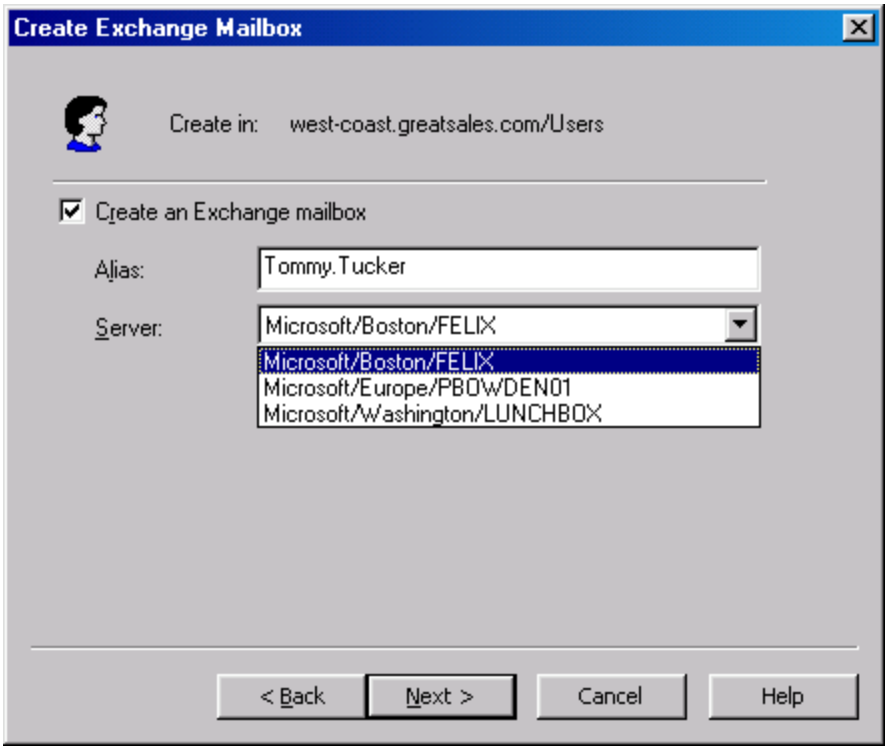
Display name	(Set to the mailbox display name)
Earlier login name	(Set to the selected logon name)

For the Active Directory to recognize the existence of an Exchange 5.5 installation, the ADC should be installed. Even if you haven't configured any CAs, the ADC should appear in the Active Directory Sites and Services Manager and all Active Directory **User** and **Contact** objects should have new configuration options:

- **E-mail Addresses** tab
- **Create an Exchange mailbox** option

On creation of **User** objects, the wizard now prompts you to create an Exchange mailbox, although if you have not configured a CA, these options are unavailable.

Note The new options available after ADC installation are supported only on servers and workstations that have the ADC manager component installed directly on them.

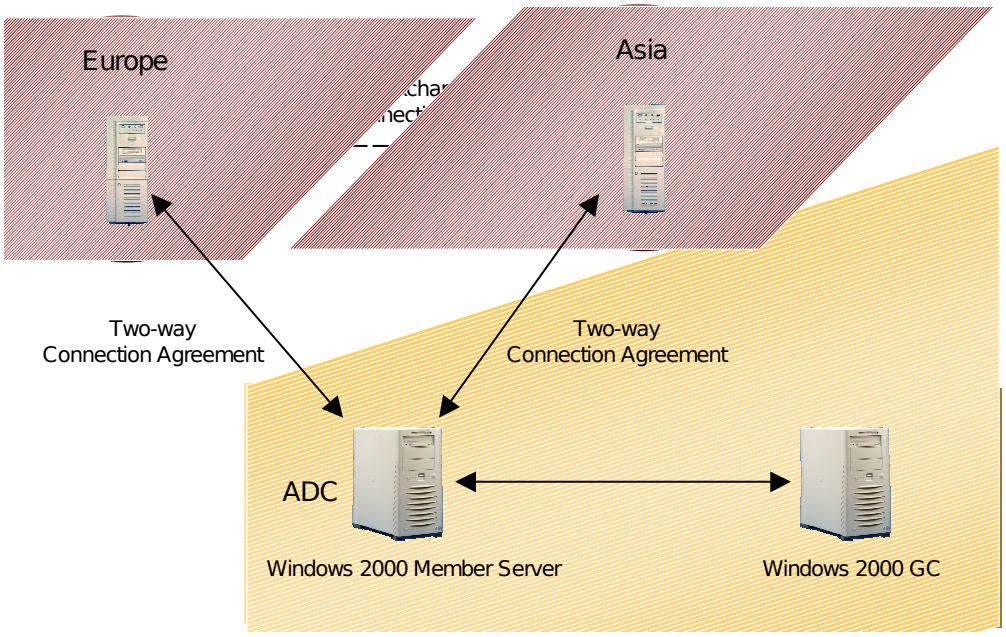


Where Should the ADC Be Installed?

Selecting the correct class of computer to run the ADC depends on the size of your existing Exchange deployment, the number of Windows 2000 domains, and the hardware budget available.

Depending on the replication schedule set for the CAs, the number of calls made into the Active Directory and the processing load can be significant. Logically, it makes sense to install the ADC service directly onto a Global Catalog server; however, considering that the Global Catalog is a precious resource in the organization, you may decide to implement the ADC on a member server, ensuring that a fast network link exists between the member and the GC. Ideally, the Exchange 5.5 bridgehead server should also be on the same fast network. This allows you to achieve the best performance from all of the components. Of course, if you deploy the ADC in this manner it may involve additional hardware costs that must be taken into consideration.

Although CAs are defined and executed on the ADC server, the source and target directories reside on other computers.



Deploying Multiple ADC Servers

You can deploy multiple ADC servers in large installations; although, you must configure the CAs so that different sets of objects are replicated by each. If only mail-based connectivity exists or if you require additional replication performance, you can deploy multiple ADC servers to ensure that Internet Protocol (IP) connections between servers are relatively local. They should not be deployed as a *fault-tolerant* solution, although you can mitigate the risk of downtime by having more than one ADC server in the enterprise.

Administration and management overhead can be kept to a minimum when you deploy multiple ADC servers because the ADC obtains all configuration information from the configuration-naming context in the Active Directory. Because each domain controller in the forest holds a read/write copy of this context, system administrators can manage CAs remotely, even if direct IP connectivity does not exist between the management console and the ADC server. In this scenario, the system administrator makes changes to a local domain controller that then replicates to all of the other servers.

LDAP Ports and Protocols

By default, the ADC server attempts to communicate with the Exchange directory bridgehead on port 389 (379 for the Site Replication Service), which is the most commonly used LDAP port. In some circumstances, you must configure the CA for another port, the obvious case being one in which Exchange 5.5 Server is deployed on a Windows 2000 domain controller. Active Directory components always start before the Exchange directory; therefore, the operating system *locks* port 389. The Exchange directory still starts, but LDAP communications are not possible. To work around this, use the Exchange 5.5 Administration program to reconfigure the listening port for LDAP (usually, port 390 is a good choice), and then set the CA on the ADC to match.

The CA does not have any LDAP port configuration for the Active Directory because it always attempts to communicate with an Active Directory server on port 3268. This is the reserved port for Global Catalog servers, which implicitly means that all CAs must be made into Global Catalog servers and not standard domain controllers.

Just about all communications that the ADC server establishes are based on LDAP. There is, however, one instance in which the ADC will use a few synchronous remote procedure calls (RPCs): when you use the Active Directory snap-in to create a **User** object, but the mailbox is specified to exist on an Exchange 5.5 server. When the next replication cycle occurs, an instance of the **Mailbox** object is created and a call is made to create new proxy addresses, such as Simple Mail Transport Protocol (SMTP), X.400, or MS. The proxy

address generator can be called only through RPC. This may be a consideration for you if a firewall exists between the ADC server and the Exchange 5.5 bridgehead.

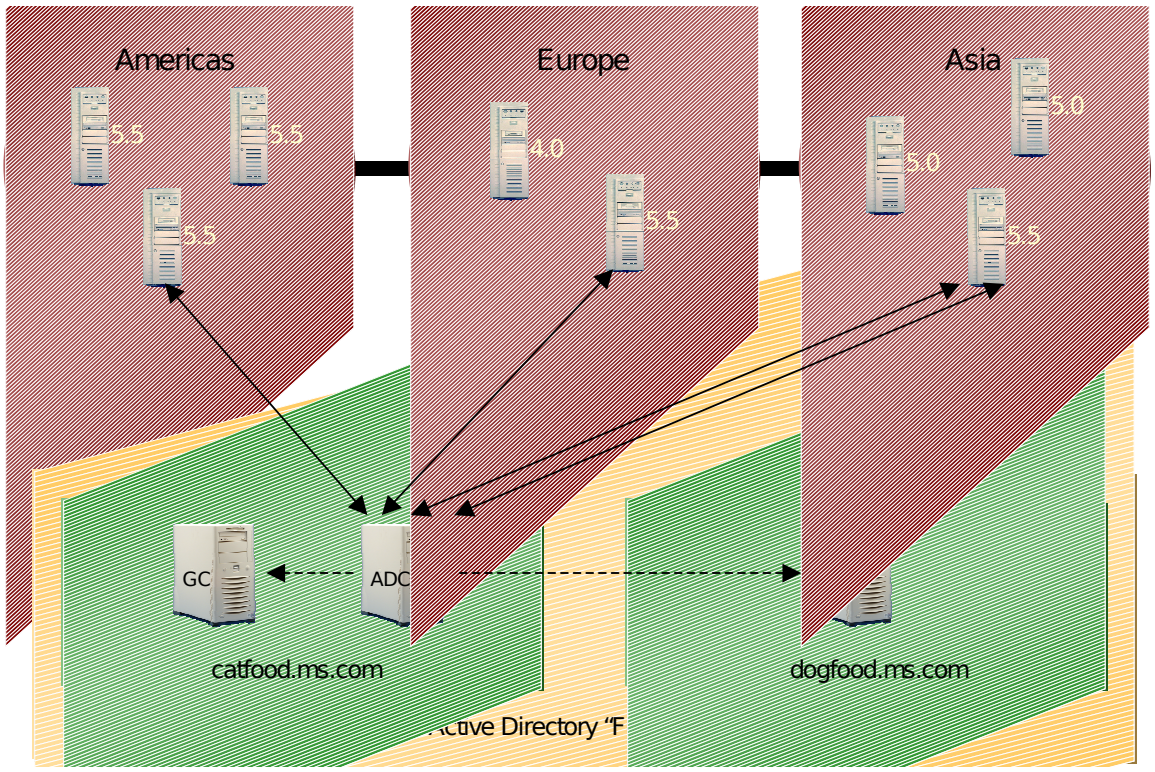
Scenario: Two Active Directory Domains, Three Exchange Sites

This scenario assumes that all Exchange mailboxes in the Americas and Europe Exchange sites, and some of the Exchange mailboxes in the Asia Exchange site have their primary Windows NT accounts mapped to the **cat.ms.com** domain. The other Exchange mailboxes in the Asia Exchange site have user accounts in the **dog.ms.com** domain, and these are in a manually created recipients container in the Exchange directory.

The scenario also assumes that each Active Directory domain has all **User**, **Group**, and **Contact** objects in the **Users** container.

Therefore, to support full two-way replication between directories (assuming good network connectivity exists), the company deploys only one ADC server. The ADC server in the **cat.ms.com** domain handles the CAs for both Active Directory domains. Although the Active Directory does not require a Global Catalog server to be present in each domain, the ADC (and other Exchange 2000 components) benefit from having fast, local access to the full Active Directory catalog. Additionally, a Global Catalog server has a full replica of its home domain but only a partial replica of the other domains within the forest, and these partial domains are read-only.

Note Because the ADC in the **cat.ms.com** domain is replicating the **Users** container to three Exchange sites, which, in turn, are replicated to each other, the **This is the primary connection to the connected Exchange Organization** checkbox must be selected on only one of the three CAs. If the primary connection checkbox is selected on more than one CA, the ADC replicates the same **Contact** and **Group** objects to each Exchange site, resulting in duplicate entries in the Exchange Global Address List.



Container Mapping

The ADC supports some fairly complex container-mapping schemes that you need to consider if either the Active Directory domain has been split into many organizational

units, or if the legacy Exchange environment uses more than one **Recipients** container. Depending on the requirements, you may need to deploy multiple CAs from the Active Directory domain to the same Exchange site.

One of the basic questions that designers ask is, "Should I map the Active Directory **Users** container to the **Recipients** container in the Exchange directory?" And following that, "Should I place legacy Exchange objects in the **Users** container?"

The container-mapping scheme you use with the ADC depends largely on your business requirements for the Active Directory and on your existing Exchange site configuration. Remember that the ADC uses the target container set on the CA to replicate directory objects that cannot be automatically mapped between the two directories; therefore, in an Exchange organization that has both Exchange 5.*x* and Exchange 2000 servers, the replicated directory objects are replicated to the correct containers automatically, and you do not need to make a decision.

The following are examples of container mapping based on different scenarios:

Scenario #1: Simple Mapping

Existing Exchange environment:

Two Exchange 5.5 sites: Reading (the largest) and Manchester, are replicated together using native Exchange directory replication connectors. Each site has only the standard **Recipients** container and this holds all **Mailbox**, **Custom Recipient**, and **Distribution List** objects. The primary Windows NT account of each **Mailbox** object currently maps to a **User** object in the Active Directory.

Business and technical requirements for the Active Directory:

- One domain called **smorg.com** and all objects residing in the standard **Users** container.
- All objects managed from a single tool.

Solution:

Deploy one ADC server. Configure one CA for each existing Exchange site.

Attribute/CA	***CA1 to Reading***	***CA1 to Manchester***
Type	Two-way	Two-way
Source Active Directory containers	**Users**	**Users**
Objects from Active Directory	**Users**/**Contacts**/**Groups**	**Users**/**Contacts**/**Groups**
Target Exchange container	Reading/**Recipients**	Manchester/**Recipients**
Source Exchange containers	Reading/**Recipients**	Manchester/**Recipients**
Objects from Exchange	**Mailboxes**/**Custom Recipients** /**Distribution Lists**	**Mailboxes**/**Custom Recipients** /**Distribution Lists**
Target Active Directory container	**Users**	**Users**

Primary CA	Yes	No

Scenario #2: Split Containers

Existing Exchange environment:

Three Exchange 5.5 sites: Boston (the largest), Washington, and Seattle are replicated together using native Exchange directory replication connectors. Each site has the standard **Recipients** container for **Mailbox** objects, but there is also a **DL** container in each site for **Distribution List** objects. In addition, the Boston site has an **Internet** container to hold SMTP custom recipients for company mail-shots. The primary Windows NT account of each **Mailbox** object in Boston and Washington maps to **User** objects in the **east-coast.greatsales.com** Active Directory domain; **Mailbox** objects in the Seattle site map to **User** objects in the **west-coast.greatsales.com** Active Directory domain.

Business and technical requirements for the Active Directory:

- Two domains, **east-coast.greatsales.com** and **west-coast.greatsales.com**, in the same Active Directory. The reason for the two domains is that the network link is very slow and prone to problems between the two coasts; therefore, SMTP replication is used between the two domains.
- The business no longer needs to split up **Mailboxes** and **Distribution Lists**, so the objects in those Exchange containers are consolidated into the Active Directory **Users** container when replicated.
- The business does, however, want to keep the SMTP custom recipients in a different organizational unit in the Active Directory, which is called **External** and will reside in the **east-coast.greatsales.com** domain.
- The Active Directory Services Interfaces (ADSI) application that has previously created custom recipients in the **Internet** container in the Boston Exchange Site has been modified to create all new addresses as **mail-enabled Contacts** within the **External** organizational unit in the **east-coast.greatsales.com domain**. However, the mail-shot application still uses the Exchange Global Address List, and so the new contact entries must be replicated to the **Internet** container in Exchange.
- No mail-enabled contacts are to be created in the **west-coast.greatsales.com** domain.
- Mail-enabled **Group** objects are created in both domains and these replicate to the existing Exchange network and go into the correct **DL** container.
- No requirement to manage all users from a separate tool. All Exchange 5.*x* **Mailbox** objects will continue to be created using the Exchange Administrator program.

Solution:

Deploy two ADC servers, one for each Active Directory domain, to avoid network link problems. For the East Coast ADC, configure two CAs to the Boston Exchange site and one to Washington. For the West Coast ADC, configure one CA to the Seattle Exchange site.

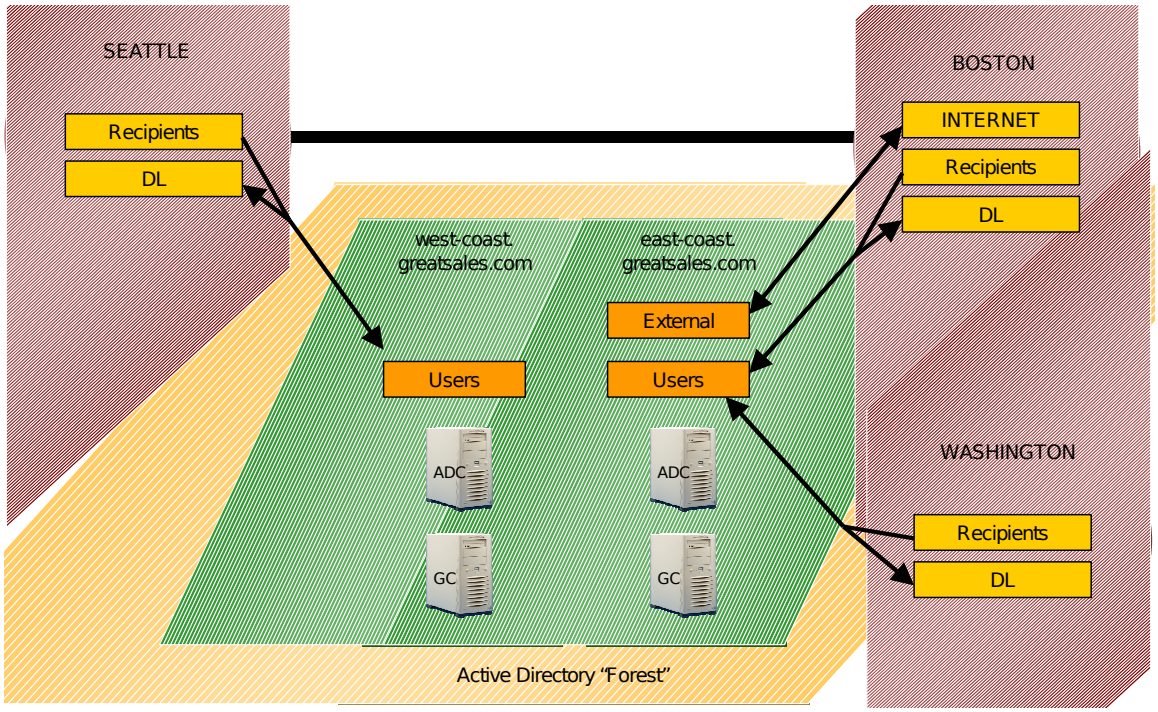
Attribute/CA	***CA1 to Boston (East Coast ADC)***	***CA2 to Boston (East Coast ADC)***
Type	Two-way	Two-way
Source Active Directory containers	East Coast/**Users**	East Coast/**External**
Objects from Active Directory	**Users**, **Groups**	**Contacts**
Target Exchange container	Boston/**DL**	Boston/**Internet**
Source Exchange containers	Boston/**Recipients** Boston/**DL**	Boston/**Internet**
Objects from Exchange	**Mailboxes**, **Distribution Lists**	**Custom Recipients**
Target Active Directory container	East Coast/**Users**	East Coast/**External**
Exchange primary CA	Yes	Yes
Windows primary CA	Yes	No

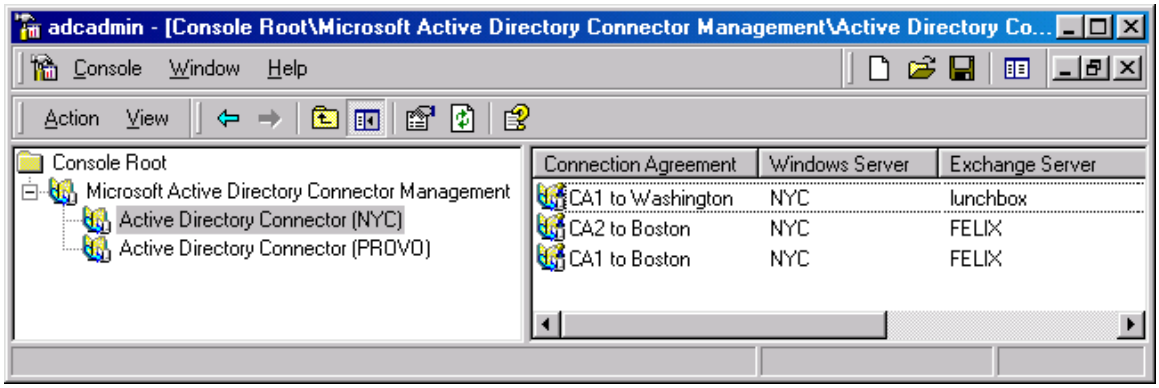
Attribute/CA	***CA1 to Washington (East Coast ADC)***
Type	Two-way
Source Active Directory containers	East Coast/**Users**

Objects from Active Directory	**Users**, **Groups**
Target Exchange container	Washington/**DL**
Source Exchange containers	Washington/**Recipients** Washington/**DL**
Objects from Exchange	**Mailboxes**, **Distribution Lists**
Target Active Directory container	East Coast/**Users**
Exchange primary CA	No
Windows primary CA	Yes

Attribute/CA	***CA1 to Seattle (West Coast ADC)***
Type	Two-way
Source Active Directory containers	West Coast/**Users**
Objects from Active Directory	**Users**, **Groups**
Target Exchange container	Seattle/**DL**
Source Exchange containers	Seattle/**Recipients** Seattle/**DL**
Objects from Exchange	**Mailboxes**, **Distribution Lists**
Target Active Directory container	West Coast/**Users**
Exchange primary CA	Yes
Windows primary CA	Yes

The following illustration is a pictorial representation of the proposed connectivity:





Explanations and notes:

Because this scenario is relatively complex, it deserves some additional explanation.

1. Both CA1 and CA2 to Boston are set as primary CAs. Under most circumstances, this would create duplicate objects; however, in this environment, each CA carries different object classes into the site, so there is no overlap.
2. The CA to Washington is not a primary CA because this conflicts with CA1 to Boston and produces duplicate objects in the Exchange directory. Therefore, all new groups created in the **east-coast.greatsales.com** domain are replicated primarily to the Boston Exchange site. Of course, these **Group** objects are available to users in all sites because Exchange directory replication is in place.

   Note You can still use Microsoft Management Console (MMC) to manage **Distribution Lists** objects that are replicated into the Active Directory from Washington because a two-way CA is defined.
3. The CA to Seattle can be set as the primary CA because the source Active Directory objects are from a different domain than the East Coast CAs.

4. This scenario assumes that all Exchange 5.5 **Mailbox** objects are created from the Exchange Administrator program. If however, new **Mailbox** objects are created using the MMC, the objects are replicated to the **DL** container in each Exchange site, which is undesirable. In circumstances in which all administration tasks must be performed by using the MMC, additional CAs are required.

Resource Usage

Server Resources Consumed by the ADC

Depending on the replication time set and the number of objects changed, the ADC server and the other directory servers it interacts with may need to process large amounts of data, so it is important that these computers have adequate power and memory and that they be not only well-connected to the rest of the network, but also, ideally, set up on the same, fast, local area network (LAN) together.

When the ADC threads are working, the load placed on the CPU of the server running the ADC is roughly 50 percent. This consumption level is constant until all replication is complete; however, the load placed on the CPUs of the computers running the directories is relatively low in comparison.

Network Consumption

For large Exchange Server and Active Directory deployments, you need to carefully plan for any additional overhead that the ADC and its Connection Agreements (CAs) produce. The following information is especially important to people who need to accurately size servers and network capacity. This information is even more important when the ADC server, Active Directory server, and Exchange 5.5 server are connected over relatively slow links.

The table below indicates the number of network frames and total traffic sent between the different components. In the following scenarios, changes are made to **User** objects in the Active Directory; in reality, the change was simply to the phone number on a directory object. Similarly, changes are made to the **phone number** field in the Exchange directory objects. In these examples, the ADC is running on a member server. If your deployment places the ADC and Global Catalog on the same computer, disregard the network communications between the ADC and Global Catalog in the table.

Test	ADC to Global Catalog	Global Catalog to ADC	ADC to Ex5/SRS	Ex5/SRS to ADC	Totals (frames and wire size)
No objects to replicate	47 frames 19 KB	36 frames 14 KB	20 frames 5 KB	16 frames 3 KB	119 frames 41 KB
One change in the Active Directory	70 frames 24 KB	89 frames 91 KB	27 frames 9 KB	24 frames 8 KB	210 frames 132 KB
Two changes in the Active Directory	73 frames 24 KB	98 frames 98 KB	34 frames 11 KB	30 frames 12 KB	236 frames 143 KB
Three changes in the Active Directory	77 frames 24 KB	96 frames 101 KB	40 frames 14 KB	36 frames 15 KB	249 frames 154 KB
One change in the Exchange Server 5.5 Directory Service	87 frames 33 KB	103 frames 103 KB	29 frames 10 KB	24 frames 8 KB	243 frames 154 KB
Two changes in the Exchange Server 5.5 Directory Service	94 frames 37 KB	114 frames 111 KB	32 frames 10 KB	27 frames 10 KB	267 frames 168 KB
Three changes in the	107	122	37 frames	30 frames	296 frames

Exchange Server 5.5 Directory Service	frames 43 KB	frames 115 KB	12 KB	12 KB	182 KB

The conclusions drawn from this information are as follows:

- When the two directories are static, only a small amount of data is passed between all components; however, the majority of this small traffic is between the ADC server and the Global Catalog.
- Changes made in the Exchange directory cause a greater amount of data to be moved over the network relative to changes in the Active Directory.
- Replication data from the Active Directory to the Exchange directory appears to be linear. When there are one or more changes to be replicated, use the following calculation:

  121 KB bind + 11 KB per changed object

- Replication data from the Exchange directory to the Active Directory appears to be linear. When there are one or more changes to be replicated, use the following calculation:

  140 KB bind + 14 KB per changed object

Using the Site Replication Service with Exchange 2000 Server

Although CAs are usually configured between the Active Directory and Exchange 5.5 directory service, you can also point the agreements at the Site Replication Service (SRS) in Exchange 2000 Server. This can be advantageous when there is a slow network link between the ADC and Exchange 5.5 bridgehead server because the replication payload on the network is much smaller.

Downstream Replication Traffic

As the CA replicates data between the two environments, the objects replicated also change, causing replication in the native directory. You must take this into account before configuring each CA.

Be aware that when you install a two-way CA between the Active Directory and an Exchange site (or a one-way CA to Exchange), the CA modifies and adds attributes to each Exchange directory object it comes in contact with. Because Exchange supports only object-based replication, those directory objects must be replicated again to the rest of the Exchange organization. For a large deployment of many Exchange sites, you should carefully plan the deployment of CAs. One method is to deploy them on weekends when there is potentially more bandwidth available on the network.

At a basic level, for each Exchange directory object changed on a server, approximately 5 KB of data is sent to all other servers within the site. For replication between sites, each object compresses to about 1 KB. For more information, see the “Microsoft Exchange Server 5.5 Advanced Backbone Design and Optimization” white paper on TechNet or on the Web at http://technet.microsoft.com/cdonline/content/complete/srvnetwk/exch/technote/backtraf.htm.

How the ADC Works

Initial Replication

When the Connection Agreement (CA) for the ADC is initially executed, the stored Update Sequence Number (USN) on the CA is set to 0; thus, the ADC functions as if the agreement is being run for the first time. Additionally, each CA has its own signature, which is computed at CA-configuration time. Active Directory objects replicated into the Exchange directory have the same **DSA-Signature** attribute as the legacy Exchange 5.5 server bridgehead, although the **Replication-Signature** attribute of the object matches the computed value of the CA's signature. When an Active Directory object is replicated into the Exchange directory, the **Object-Version** attribute, which is standard to Exchange, is either set to 1 (if it is a new object), or incremented by 1 (if a modification is taking place).

Before the Lightweight Directory Access Protocol (LDAP) write is made, the current value of the **Object-Version** (if it exists) is read, incremented by 1, and then written into the **Replicated-Object-Version** attribute also on the Exchange directory object. Thus, if the ADC has just modified an object, both the **Object-Version** and **Replicated-Object-Version** attributes are the same.

Detecting Changes in the Exchange Directory

When an LDAP search to the Exchange directory is performed, the request is for objects from the stored USN (on the CA) to the highest USN in the Exchange directory. This also includes tombstoned entries (that is, entries of objects that have been deleted). Additionally, a filter is set so that objects that have the signature of the CA are not requested unless the **Object-Version** attribute is greater than the **Replicated-Object-Version** attribute; this prevents the ADC from back-replicating unchanged objects previously sent to the Exchange directory.

Detecting Changes in the Active Directory

The Active Directory uses attribute-based replication, unlike the Exchange directory, which uses object-based replication. To detect changes in the Active Directory that need to be replicated to the Exchange environment, the CA uses a combination of Active Directory USNs and the sum of **Attribute Versions** of each Active Directory object in the source container.

Object Class Mapping and Attributes

The following points will help you understand how different classes of objects are mapped between the two directories:

- An Exchange 5.5 **Mailbox** object mapped to a Windows NT 4.0 account appears in the Exchange directory as a **Mailbox** object but maps to the Active Directory as a **disabled Windows User**. This default behavior of the CA can be changed to either **enabled User** or **mail-enabled Contact** in the configuration interface for the CA.

Note In versions of the ADC shipped with Exchange 2000 Beta 3 and later, you can prevent the ADC from creating an object altogether if the Exchange directory object cannot be mapped to the Windows 2000 Active Directory.

- An Exchange 5.5 **Mailbox** object mapped to an Active Directory account appears in the Exchange directory as a **Mailbox** object, and maps to the Active Directory as a **mailbox-enabled User** (the **msExchHomeServerName** attribute is set). The **Object-GUID** attribute of the Exchange **Mailbox** object is set to the globally unique identifier (GUID) of the Active Directory object, and the **legacyExchangeDN** attribute of the Active Directory object is set to the Distinguished Name (DN) of the

correlating object in the Exchange directory. All directory attributes from the two objects, such as telephone number, postal address, and so on, are merged and populated to both directory objects.

- A **Distribution List** object in the Exchange directory appears in the Active Directory as a **mail-enabled Group** object (type: **Distribution**, scope: **Universal**). Because the **DL** object may appear in the Active Directory before the membership objects exist, any orphaned members are binary encoded and written to the **unmergedAtts** attribute in the corresponding entry of the **Group** object. This ensures that membership changes to the Active Directory **Group** object successfully replicate back to the Exchange directory. The unmerged attributes are removed and resolved only after a full replication of the object is initiated.
- A Custom Recipient (of any address type) in the Exchange directory appears as a **mail-enabled Contact** in the Active Directory.

For a list of objects replicating from the Active Directory to the Exchange directory, see the following fidelity class table.

Active Directory object	***Exchange object class mapping***
Mailbox-enabled **User**	Mailbox
Mail-enabled **User**	Custom recipient in the target container
Non-mail-enabled **User**	*Not replicated*
Mail-enabled **Contact**	Custom recipient in the target container
Non-mail-enabled **Contact**	*Not replicated*
Mail-enabled **Group** (type: **Distribution**)	Distribution List in the target container
Mail-enabled **Group** (type: **Security**)	Distribution List in the target container
Non-mail-enabled **Group** (type: **Distribution**)	*Not replicated*
Non-mail-enabled **Group** (type: **Security**)	*Not replicated*

Duplicate Object Detection

If at any point the ADC attempts to create an object that already exists in the target directory, a numeric value, prefixed with a hyphen, is appended to the common name of the object. The prefix ranges from -1 to -9999.

Schema Discovery

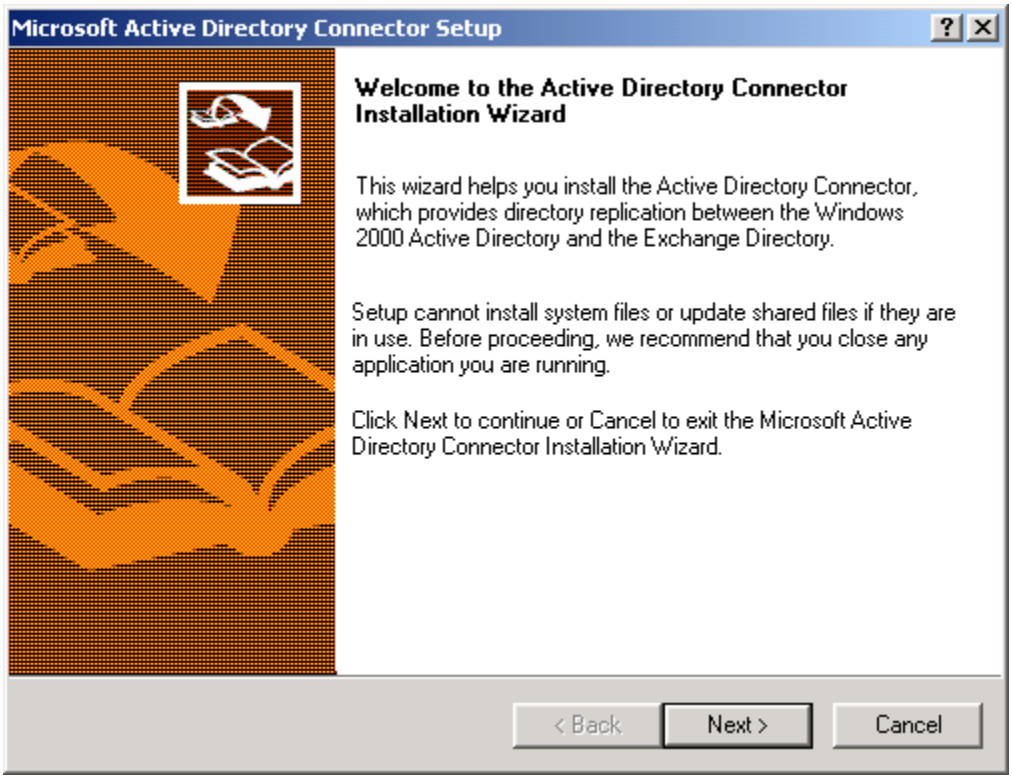
When replicating data between two different systems, the format and restrictions for the data may be different for each system; for example, the Active Directory supports UTF8 in the object name, but the corresponding entry in the Exchange directory, in this case, the DN, supports only *teletext* characters. Schema discovery allows the ADC to work out the restrictions imposed by the target directory and perform the necessary conversion. Schema discovery is designed to accommodate the following discrepancies:

- Data format and presentation (for example, UTF8 and teletext)
- Field length restrictions
- Mandatory and optional attribute mapping
- Single-value to multi-value field mappings (and vice versa)

Implementation Walkthrough

ADC Installation

1. Start ADC Setup. You can find the ADC Setup program in the \Valupack\mgmt\adc directory on the Windows 2000 Installation CD or in the \Adc\i386 directory on the Exchange 2000 CD.

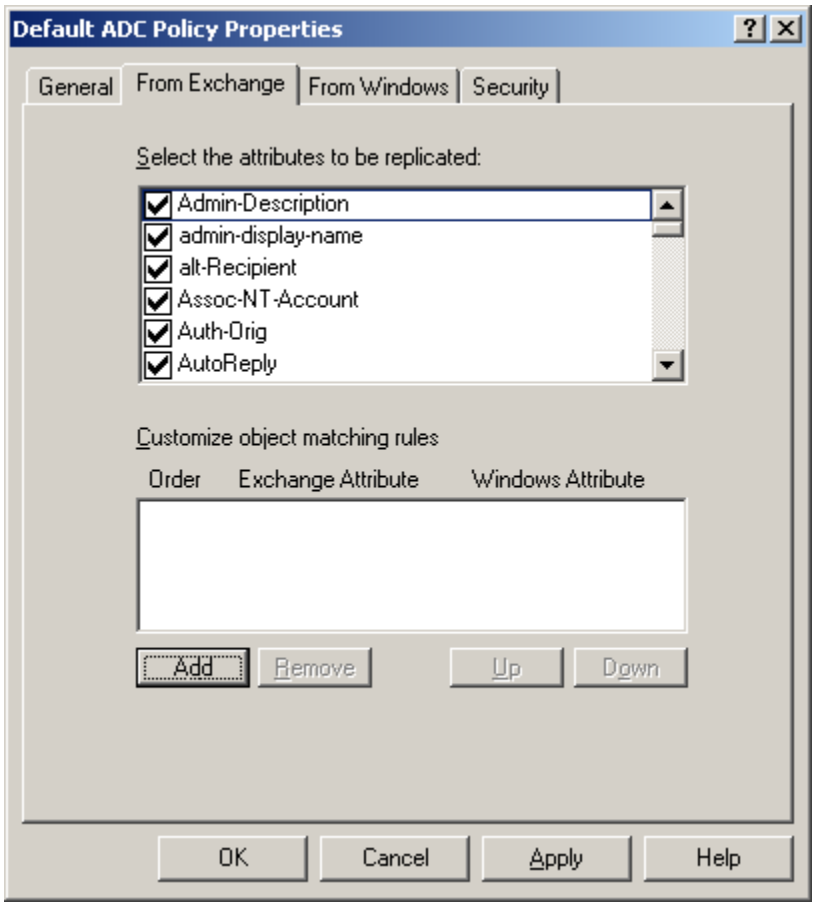

Microsoft Active Directory Connector Setup
Welcome to the Active Directory Connector Installation Wizard
This wizard helps you install the Active Directory Connector, which provides directory replication between the Windows 2000 Active Directory and the Exchange Directory.
Setup cannot install system files or update shared files if they are in use. Before proceeding, we recommend that you close any application you are running.
Click Next to continue or Cancel to exit the Microsoft Active Directory Connector Installation Wizard.
< Back
Next >
Cancel

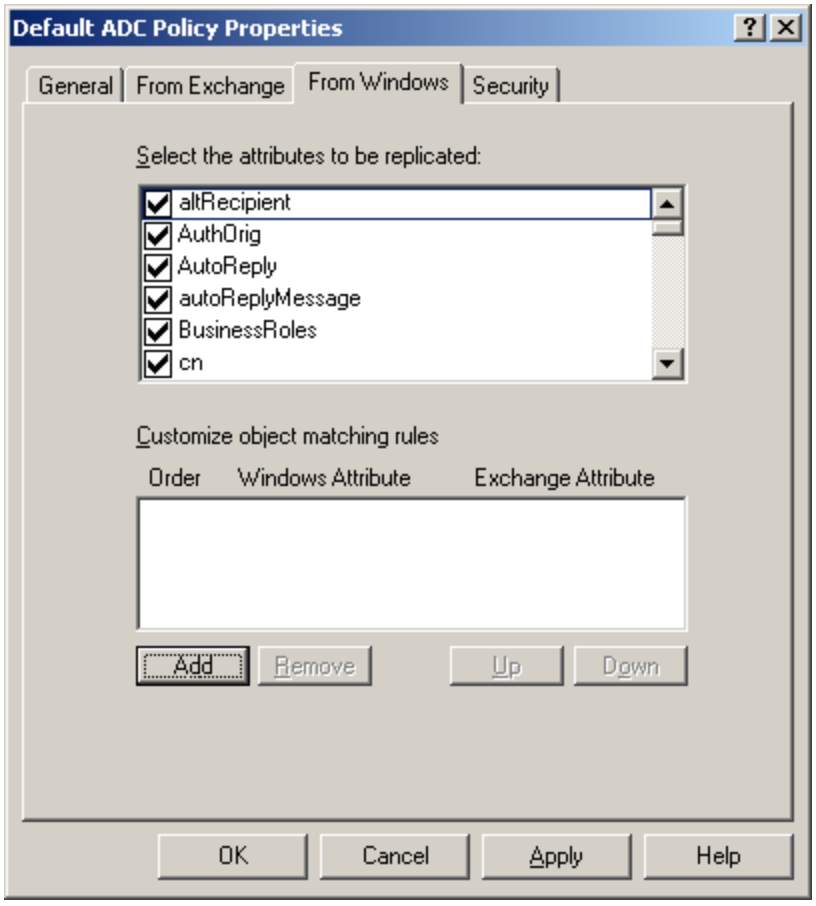
2. Install both the Connector and Manager.
3. Enter the installation directory.
4. Enter the Site Services Account name and password.

Configuring Attribute Replication and Object Matching

You may have business and technical reasons for not wanting all attributes to be replicated on objects between the Exchange and Active Directory. To hide certain attributes from replication, use the property sheets of the ADC.

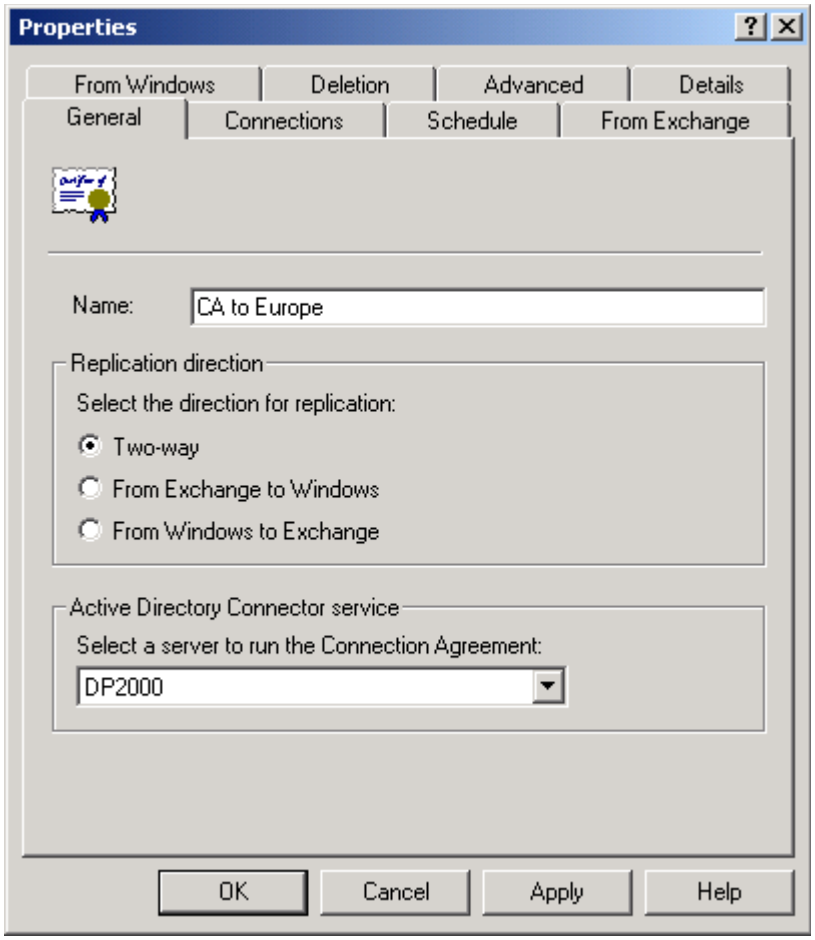
Additionally, by default, the ADC attempts to match objects between the two directories based on the **NT-security-descriptor** field. In the majority of cases, this default is fine; however, in other situations you might want to change the attribute mappings (for example, match the Exchange alias name to the Active Directory user name). Not only can you specify the attribute-mapping rules, but you can also define an ordered list of rules.


Default ADC Policy Properties
General
From Exchange
From Windows
Security
Select the attributes to be replicated:
Admin-Description
admin-display-name
alt-Recipient
Assoc-NT-Account
Auth-Orig
AutoReply
Customize object matching rules
Order
Exchange Attribute
Windows Attribute
Add
Remove
Up
Down
OK
Cancel
Apply
Help


Default ADC Policy Properties
General
From Exchange
From Windows
Security
Select the attributes to be replicated:
altRecipient
AuthOrig
AutoReply
autoReplyMessage
BusinessRoles
cn
Customize object matching rules
Order
Windows Attribute
Exchange Attribute
Add
Remove
Up
Down
OK
Cancel
Apply
Help

Creating a Connection Agreement

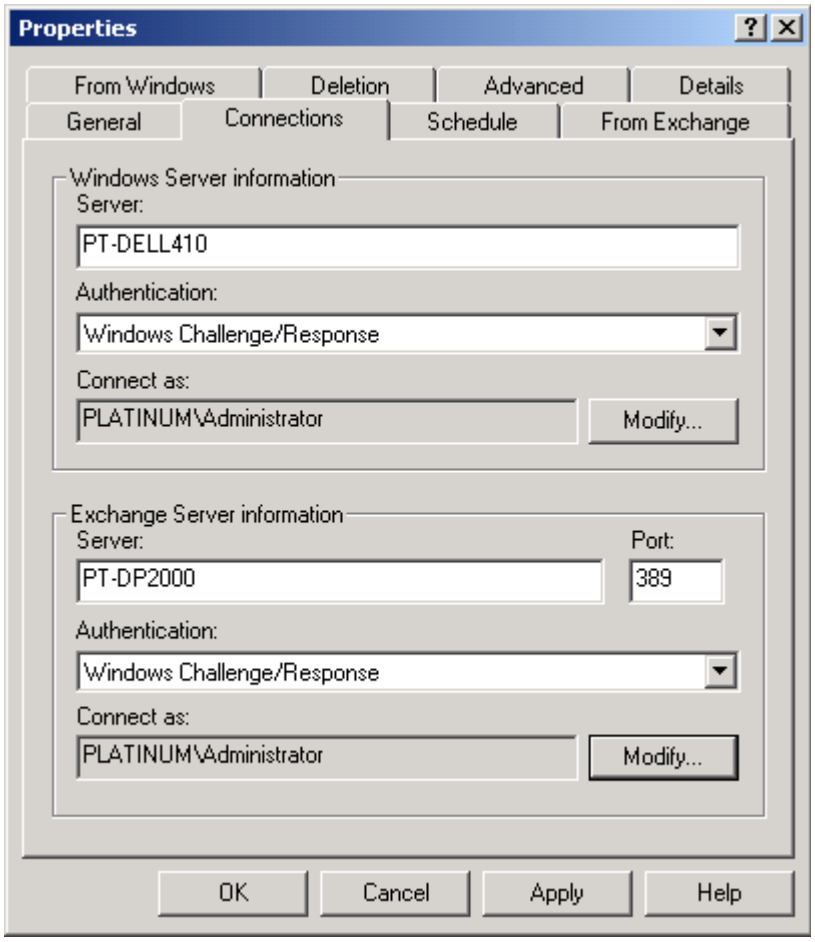
1. Open the Exchange Active Directory Connector Microsoft Management Console (MMC) and choose to create a new Connection Agreement (CA).



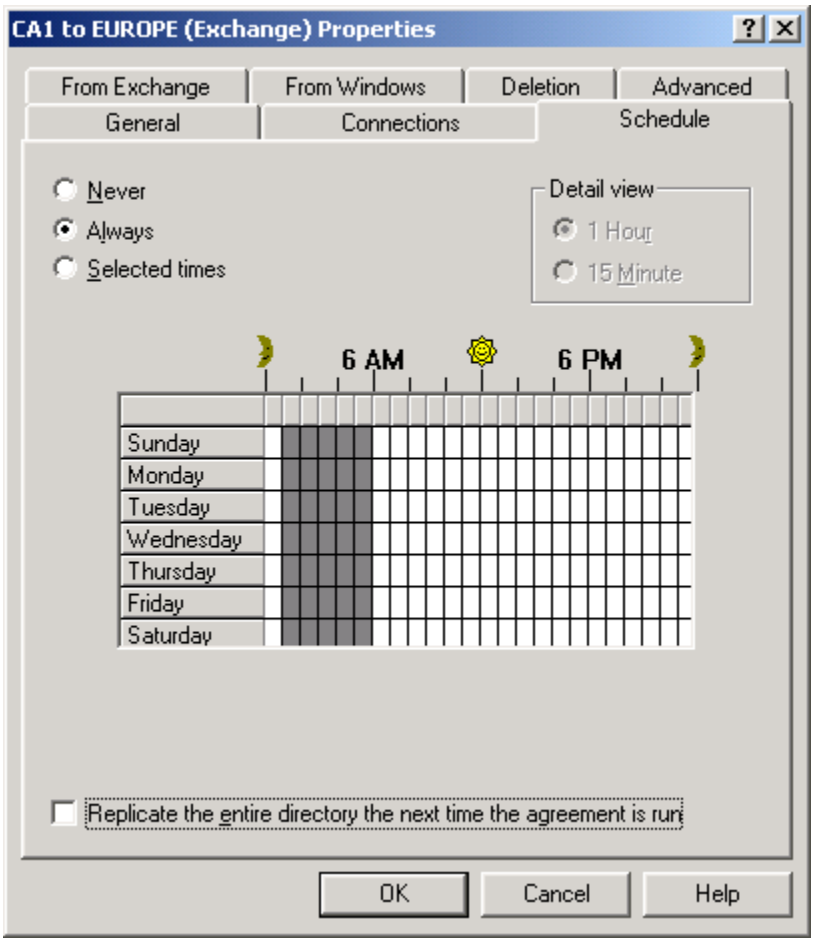
You will need to enter details, such as whether the agreement is one-way or two-way, and specify the server to run the ADC. In most circumstances, this will be the local server.

2. Enter the connection information (this includes the source and target directory servers, plus logon credentials and authentication type). If the ADC is installed on a member server, specify the local Global Catalog as the source Windows NT server.

   You may also need to change the Lightweight Directory Access Protocol (LDAP) port for the Exchange directory if the default has been changed on the Exchange server. This can be verified by looking at the LDAP protocol in the Protocols container in the Exchange Administrator program.



3. Select the activation schedule for directory replication. During active hours, the CA checks for and processes changes once every 5 minutes. Additionally, the setting of **Always** equates to every 5 minutes, 24 hours a day, 7 days a week (previous releases of Exchange Server used **Always** to indicate every 15 minutes). Because the ADC CA is most often used for mixed-vintage Exchange sites, the 5-minute period aligns with the normal intra-site directory replication latency timer.



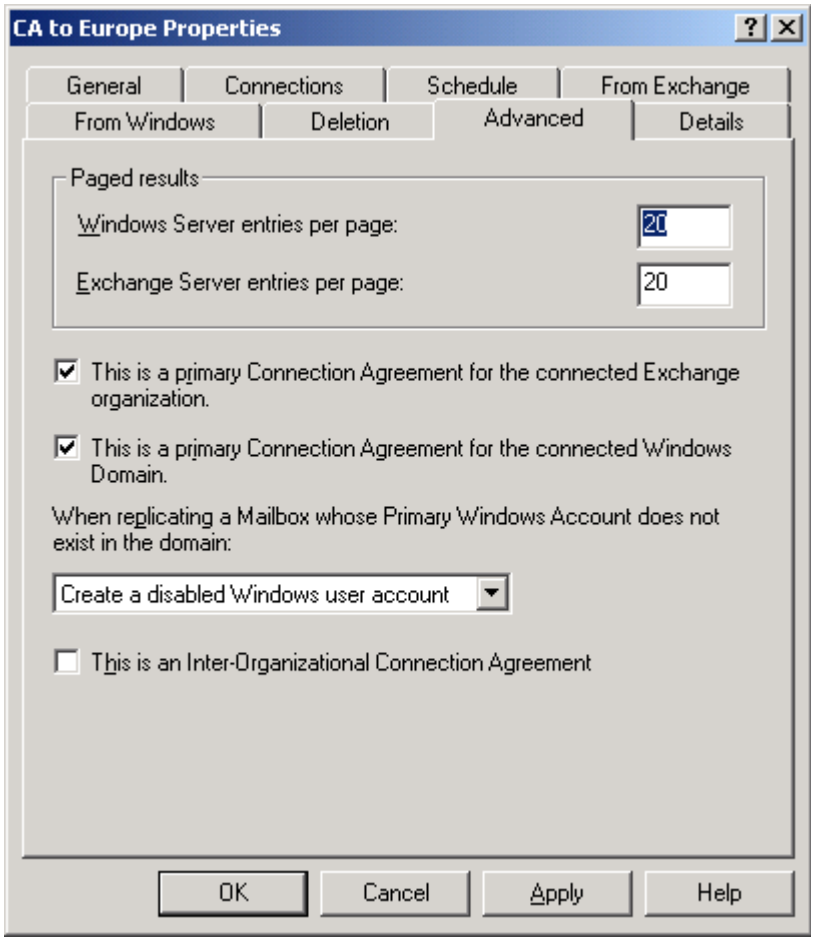
Selecting the **Replicate the entire directory** checkbox sets the following attributes on the CA:

msExchServerXHighestUSN 0

msExchDoFullReplication True

This requires all directory objects to be checked for consistency. If there are any discrepancies between the directories, objects are replaced as appropriate; however, if objects are consistent, they are not replicated again.

4. Click the **Advanced** property tab. The settings on this tab determine the finer details of how the ADC works.



Usually, you do not need to change LDAP page sizes. Although the default of 20 entries per paged result appears to be quite small, it paces the processor to be kept continually busy while receiving changes, rather than overly busy or not at all busy.

The other options on the **Advanced** tab are very important. The checkboxes indicating primary Connection Agreements, or *bridgehead bits* as they are known, control what happens when replication cannot find a match between associated objects in the two directories. Although the two checkboxes look similar, they perform slightly different functions:

This is the primary Connection Agreement for the connected Exchange organization

You can configure multiple CAs in the Exchange environment; and this is particularly important when you have multiple sites and require two-way replication. Imagine, though, that the Active Directory source for those CAs is the same container or organizational unit. This means that each CA replicates, by default, the same objects (such as **Groups** and **Contacts**) to each site. If those Exchange sites are also replicated together, duplicate entries appear in the Global Address List;. therefore, by

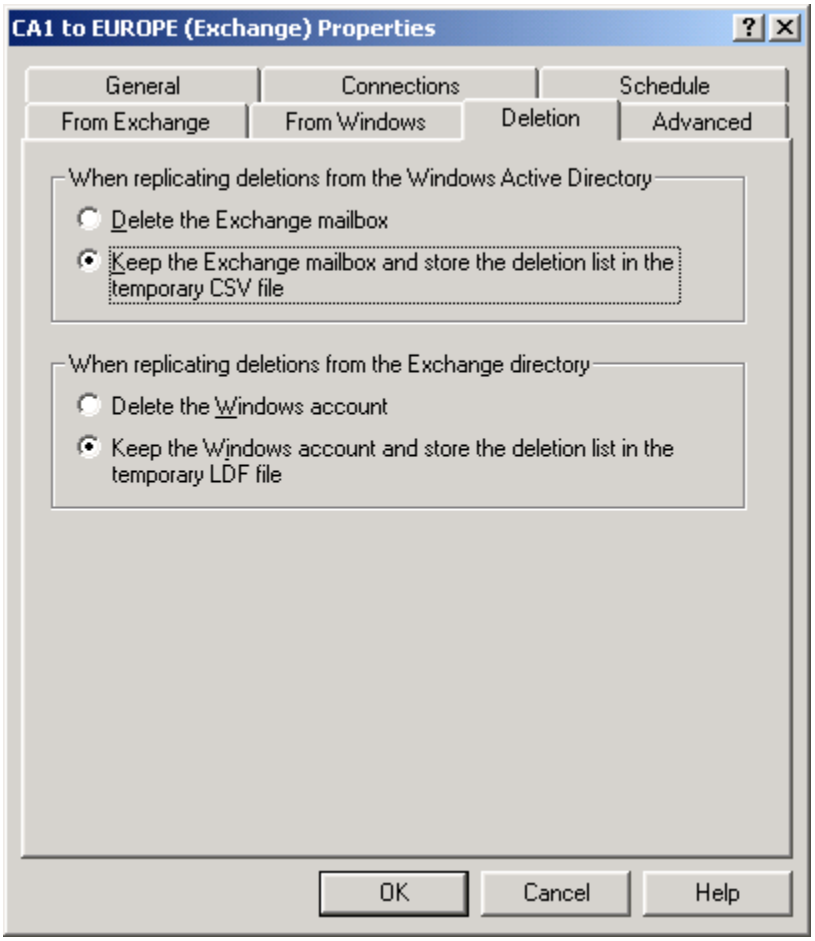
clearing this checkbox, the CA replicates only changes to objects that already exist in the Exchange directory. New objects including **Group** and **Contacts** are not replicated through this CA.

It is not entirely accurate to say that you should not have more than one primary CA for each Exchange organization because this depends on the source containers or organizational units selected in the Active Directory and the object classes being replicated by each agreement. For multiple Active Directory domain environments, you should have more than one primary agreement, so that objects other than **User** objects are represented in the Exchange directory.

This is the primary Connection Agreement for the connected Windows Domain

Associated with this checkbox is the setting for replicating a **Mailbox** object that has no existing primary Windows NT account. Implicitly, this checkbox controls whether an object is created in the domain if a match cannot be found. Clearing this checkbox makes the drop-down list unavailable. You can use this option you need to replicate an entire container from the Exchange environment and know that some of the **Mailbox** objects do not have Active Directory accounts in the Windows 2000 domain. Instead of allowing the ADC to create contacts or new user accounts, this option sets the ADC to not represent those objects at all.

5. Click the **Deletion** tab. The settings on this tab determine the action when directory objects are removed from source and target directories.


CA1 to EUROPE (Exchange) Properties
General
Connections
Schedule
From Exchange
From Windows
Deletion
Advanced
When replicating deletions from the Windows Active Directory
Delete the Exchange mailbox
Keep the Exchange mailbox and store the deletion list in the temporary CSV file
When replicating deletions from the Exchange directory
Delete the Windows account
Keep the Windows account and store the deletion list in the temporary LDF file
OK
Cancel
Help

By default, objects deleted from each directory are not propagated to the target. Instead, the deletions are held in the following directories on the ADC server:

\<%windir%>\MSADC\Connection Agreement name

Win2000.ldf	Entries deleted from the Exchange directory
Ex55.csv	Entries deleted from the Active Directory

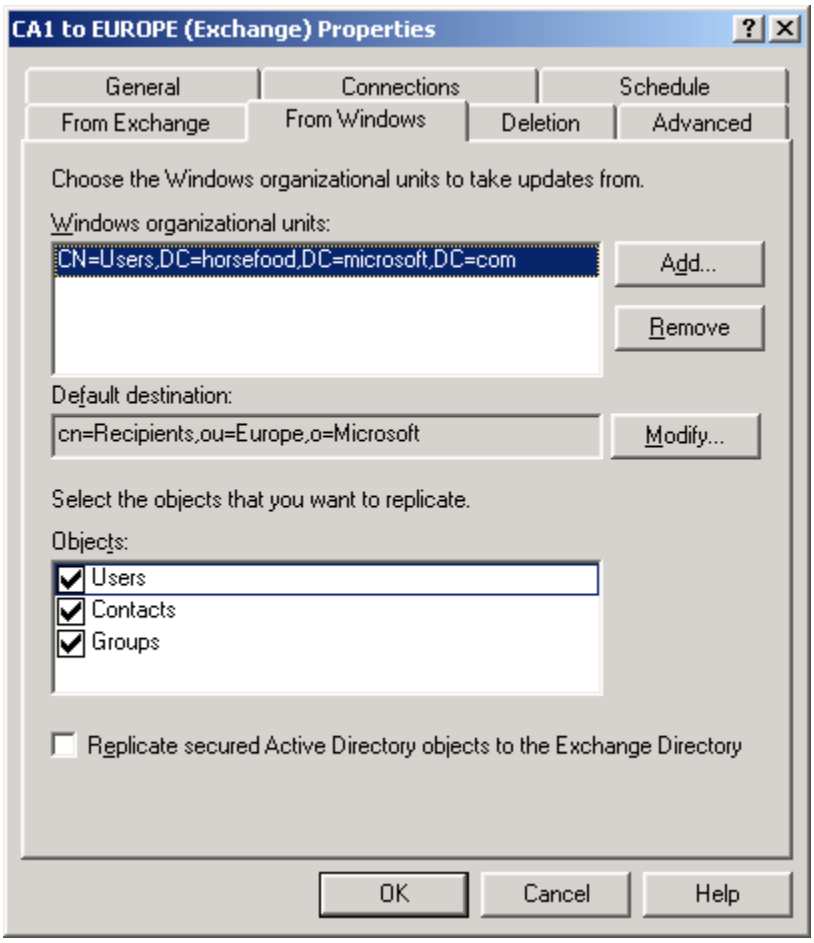
Opting not to propagate deletions can cause additional management overhead because the system administrator must look through the created files and import them into the adjacent directory. If there are several hundred changes occurring and you have tight control over who can delete **Directory** objects, you may opt to enable deletion propagation.

If you decide to enable deletions through the user interface, be very careful of the changes that you make to each directory; for example, deleting a **Custom Recipient** object in Exchange deletes the related Active Directory object, which may be a mail-enabled **Contact** or **User** object representing an account from a different domain.

Note System administrators may want **Contact** object deletions to be propagated, but they may not want **Mailbox** object deletions to be propagated. To improve the granularity of deletion control in Exchange 2000 Server Beta 3, you can configure multiple CAs with different options.

---

6. Click the **From Windows** tab. The settings on this tab determine which containers or organizational units are sent to the Exchange directory and specify the default destination container where they are received in the Exchange 5.5 site. If a complex hierarchy exists within the Active Directory domain, it is not necessary to select each organizational unit individually; you can select the top-level domain as the source. However, this assumes that you want to retain that hierarchy; when replicating to Exchange, those containers are automatically created by the ADC.

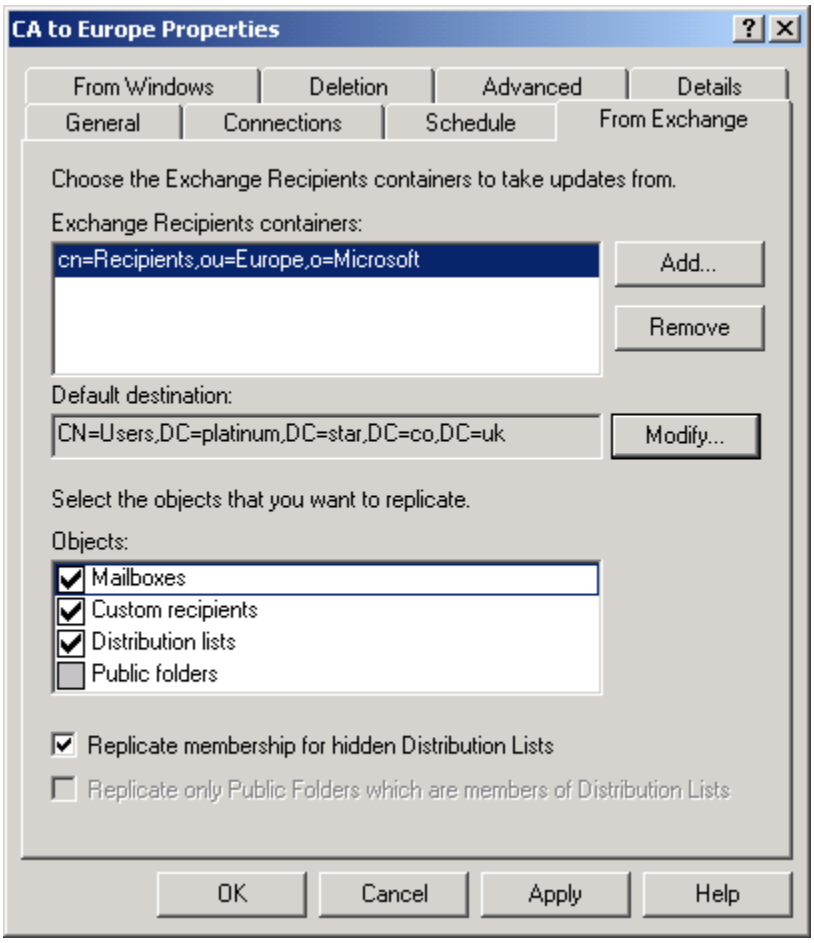


The default concept is important to understand. If an Active Directory **User** object is mapped to a **Mailbox** object in the **Recipients** container, and the CA specifies that objects be sent to a different Exchange container, a duplicate object is not created in Exchange. The ADC retains the relationship between the two objects correctly; therefore, think of this option as, "If the Active Directory object does not relate to any existing Exchange object, then an object is created by the ADC in the target container."

For example, if a mail-enabled **Contact** object is created in the Active Directory, a Custom Recipient entry appears in the target Exchange container because no mapping is achieved for security identifiers.

You can also select the object classes to replicate to the target directory.

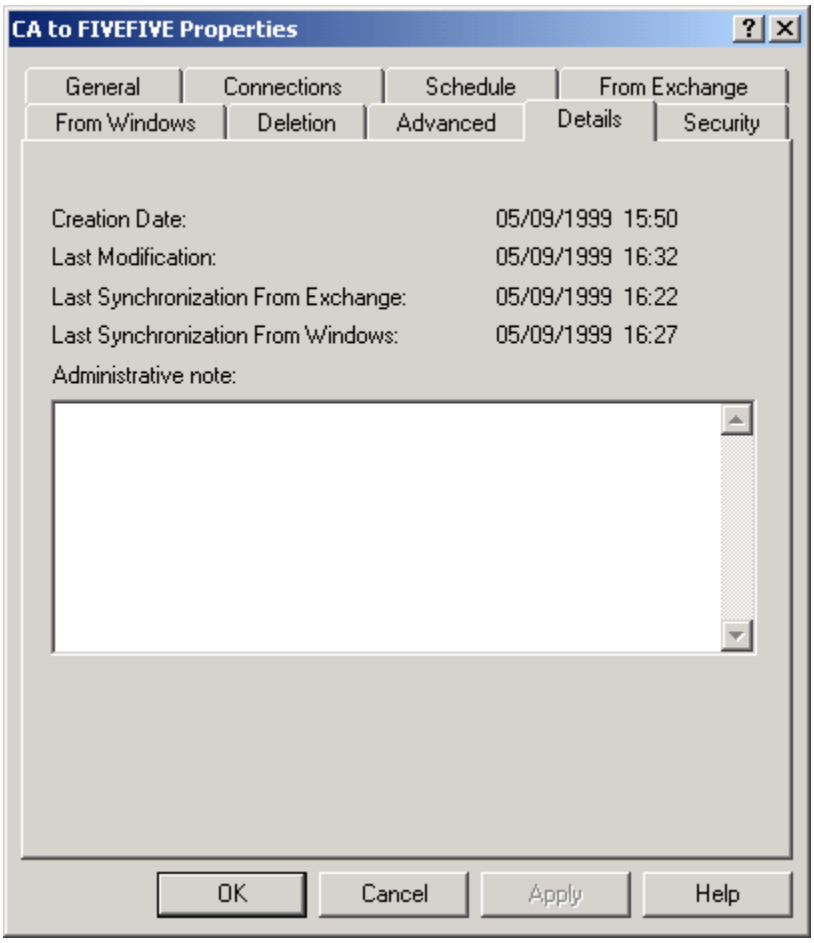
7. Click the **From Exchange** tab. The settings on this tab specify which containers to pull from the Exchange directory.



To replicate all containers on the site, select the **Site** object as the source and specify the destination container in the Active Directory and the different types of object classes to replicate from the Exchange directory. As with the **From Windows** tab described earlier, this option specifies the default target container for objects that cannot be mapped.

The option **Replicate only Public Folders which are members of Distribution Lists** is disabled unless the Connection Agreement is marked as **Inter-Organizational** on the **Advanced** tab. Unlike Exchange Server 5.5, Public Folders do not need a directory object to represent them, but to send mail to a Public Folder they must be mail-enabled, which means they must have an object in the directory. When the checkbox is cleared for this option, all Public Folder directory objects in the Exchange 5.5 site will be replicated to Active Directory. When the checkbox is selected, only Public Folders that are members of a **Distribution List** object are replicated.

8. Only containers from one Exchange site can be selected in a single CA if the agreement is configured to write to the Exchange directory. If multiple Exchange sites are deployed, you also need to establish multiple CAs.
9. Start the ADC. You can start the ADC from the Computer Management MMC or from a command prompt by typing **net start msadc**.
10. Once the ADC starts, new objects are populated in both the Active Directory and the Exchange directory. To monitor the progress of a CA, either look at the performance monitor counters or enter the properties of the agreement and choose the Details tab.



11. From here, you can create additional CAs and enable them without having to stop and restart the MSADC service; changes are implemented dynamically.

Post Installation

Replicated Objects in the Active Directory

After initial replication occurs, Exchange objects, such as **Custom Recipients**, **Distribution Lists**, and **Mailbox Agents** (for example, the Schedule+ Free/Busy Connector), are represented by objects of the same class in the Active Directory target container. A custom recipient is created in the Active Directory as a mail-enabled **Contact** object, and the **E-Mail** address field is set to the Simple Mail Transport Protocol (SMTP) proxy address of the object, even if it is a non-SMTP custom recipient. The attributes of Exchange **Mailbox** objects, if previously mapped to Windows 2000 accounts, are replicated to the associated mailbox-enabled **User** object, regardless of which container it is in.

For example, before you installed the ADC, the Exchange mailbox for Scott Cooper existed and was assigned to a **User** object. At this stage, only a display name and a downlevel login name existed for the **User** object in the Active Directory. After replication by the ADC, the **User** object contains values for all of the Exchange **Mailbox** object attributes, such as postal address, title, company, proxy addresses, Distribution List membership, and management reporting. A closer look at the **User** object reveals that an **Exchange** tab now exists and shows the Home Server as *org/site/server*. Also, the e-mail address of the object is now set to the SMTP proxy address of the Exchange mailbox.

With the correct tools, it is possible to view the raw attributes of the **User** object. Good tools for doing this include **Ldp** (Ldp.exe) and the **Active Directory Services Interface** editor (Adsiedit.dll), both of which can be found on the Windows 2000 Server Resource Kit.

Now that the ADC has properly linked an Exchange 5.5 **Mailbox** object with the Active Directory, the **User** object has many new fields:

legacyExchangeDN

/o=ORG/ou=SITE/cn=Recipients/cn=RDN

msExchHomeServerName

/o=ORG/ou=SITE/cn=Configuration/cn=Servers/cn=SERVER-NAME

replicationSignature

Set to the unique signature on the Connection Agreement (CA).

Replicated Objects in the Exchange Directory

If you specified a target container other than the standard **Recipients**, you now will see nonmapped objects, such as mail-enabled **Contacts** and **Distribution Groups**, in that container. Mailbox-enabled **Users** objects are replicated to the correct recipients container.

Exchange objects affected by the ADC will also contain some new or changed attributes, including:

ADC-Global-Names (New)

Blank by default.

DSA-Signature (Modified)

*Set to the **Invocation-ID** of the Exchange 5.5 bridgehead specified in the CA.*

Object-GUID (New)

*Set to the **objectGUID** attribute present on the **User** object in the Active Directory.*

Object-Version (Modified)

Incremented by one after the initial replication.

Replication-Signature (New)

Set to the unique signature of the CA that made the change.

Replicated-Object-Version (New)

*Matches the **Object-Version** attribute because the ADC made the last change to the object.*

Attributes of the Connection Agreement

Use the **Ldp** (Ldp.exe) utility to look at the raw attributes of the CA in the ADC. Here's the binding path:

cn=Name of CA,cn=Active Directory Connections,cn=Microsoft Exchange, cn=Services,cn=Configuration,dc=domain,dc=domain

The CA will have a number of properties, the most interesting are listed below:

msExchReplicateNow

A Boolean value. If True, the ADC performs a replication cycle immediately for this CA. This flag is usually set by the ADC administration snap-in. Because it exists within the configuration-naming context that is replicated around the forest, it is possible to set this value remotely.

msExchServer1HighestUSN

The highest update sequence number last found in the Active Directory.

msExchServer2HighestUSN

The highest update sequence number last found in the Exchange directory.

msExchDoFullReplication

A Boolean value. If True, the two directories are refreshed.

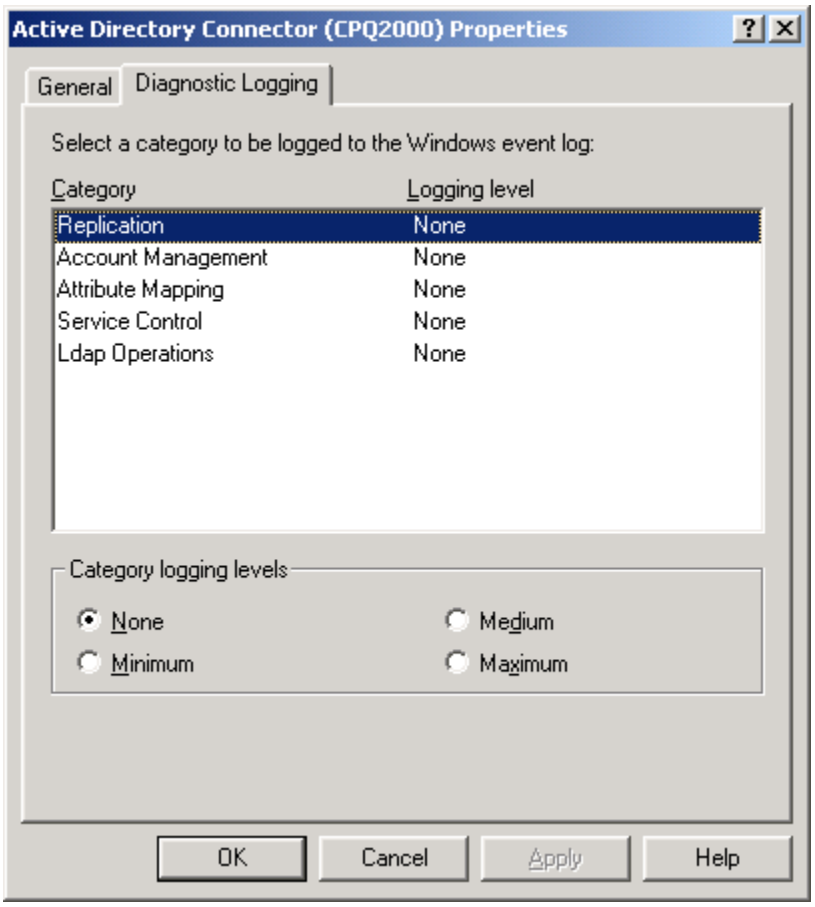
USNChanged

The Update Sequence Number (USN) assigned to the CA object at last update.

Troubleshooting

Event Logs

If you find that operations are failing to complete, you can increase the logging level for several categories. This generates more information in the Event Log. To change diagnostics logging options, go to the ADC administration snap-in for the ADC server that requires troubleshooting, and click **Diagnostic Logging**.



Time Synchronization

One of the most common problems you will come across with the ADC is that time is slightly adrift between the Exchange 5.5 and Global Catalog server; for example, an object is created, the ADC attempts to replicate it; but the adjacent directory may not have reached the time of the object creation. In this instance, the new or updated object is rejected and an 8139 replication event is logged in the Application Log.

Directory Inconsistencies

It seems that a natural reaction for resolving replication problems is to tear down connections and start again. Although in some systems this is a safe operation, in this system *extreme caution* is recommended if you destroy a Connection Agreement (CA) and then reestablish it. If there appear to be minor discrepancies between the two directories when there should not be, open the Active Directory Connector snap-in, select the CA in question, and on the **Task** menu, click **Replicate now**. If this does not resolve

the issue and only one of two objects appears to be out of date, try modifying one of the attributes on the object.

If there are major directory inconsistencies, try selecting the **Replicate entire directory** checkbox for each CA.

If for some reason, you need to tear down and reestablish CAs, do not enable deletions on the replacement CA, especially if you have removed foreign directory objects from each directory. The ADC replicates tombstones, which results in the deletion of all objects within the directory.

Advanced Configuration

Do I Need Anything Else?

In the majority of deployments, the configuration of the Connection Agreements (CAs) allowed through the Microsoft Management Console (MMC) interface is sufficient for both small and large deployments. However, where there is a very complex Exchange site or Active Directory topology, some low-level customizations to the ADC can be made. This section details two of the most common requirements.

It is important that you thoroughly test and document any customizations of this type to ensure good supportability. In addition, ensure that Microsoft support staff knows about the changes that you have made if you call Microsoft about problems with Exchange 2000 Server.

Tools

A variety of tools are available to make the configuration changes detailed in this section. Two of these tools are the **Ldp** (Ldp.exe) utility and the **Active Directory Services Interface** editor (Adsiedit.dll). Both of these tools are included in the Windows 2000 Server Resource Kit.

To use the Active Directory Services Interfaces (ADSI) editor, you must first register the Adsiedit.dll library (as an in-process server) by using Regsvr32.exe, and then open Adsiedit.msc, which is an MMC snap-in. The ADSI editor provides a graphical user interface, which is easy to use; but it is not as powerful as the **Ldp** utility.

To use the **Ldp** utility, use the **Connect** option to contact the Active Directory server, and then **Bind** to the Active Directory as an administrator account. Once authenticated, on the **View** menu, click **Tree**, and then type the Lightweight Directory Access Protocol (LDAP) path to the configuration-naming context; for example, if the domain name is **star.co.uk,** the LDAP path to type is:

cn=Configuration,dc=star,dc=co,dc=uk

To expand and collapse subcontainers and their object members, double-click containers in the left pane. To locate the Active Directory Connector resources, expand the **Services** node, then **Microsoft Exchange**, and finally **Active Directory Connections**.

Changing the LDAP Search Filter Rule

When configuring a CA, you can set the object class to be included in the replication cycle; this includes **Mailboxes**, **Custom Recipients**, **Distribution Lists**, **Users**, **Contacts**, and **Group** objects. When you make this selection, you set an attribute on the CA called **msExchServer*X*SearchFilter**, in which *X* equals 1 for the Active Directory and 2 for the Exchange directory. This string represents an RFC2254 rule (LDAP search filter). When you look at this attribute by using a tool, such as **Ldp**, you see the following:

msExchServer1SearchFilter (Active Directory)

(|(objectclass=*user*)(objectclass=*contact*)(objectclass=*group*))

msExchServer2SearchFilter (Exchange directory)

(|(objectclass=*organizationalPerson*)(objectclass=*remote-address*)
(objectclass=*groupOfNames*))

The rules query for all recipient objects in the directory (*organizationalPerson* is a **Mailbox**, *remote-address* is a **Custom Recipient**, and *groupOfNames* is a **Distribution List**). The vertical bar, or pipe, at the beginning of the string indicates this is an OR filter. For more information about LDAP search filters, see Appendix A, “RFC2254–LDAP Search Filters” in “PT102 – Exchange 2000 Server Directory Access and Integration with Windows 2000.” With tools such as **Ldp**, you can modify this rule so that the CA uses a more granular search criteria when replicating objects between the two directories. For

example, you can configure a specific CA to replicate the Exchange **Mailbox** objects in the Sales and Marketing departments to the Active Directory:

(&(objectclass=organizationalPerson)(|(department=Sales)(department=Marketing)))

Or you can have a CA that replicates only users whose last name starts with the letter A:

(&(objectclass=organizationalPerson)(sn=a*))

Changing the Attribute Map

By default, the ADC uses its own rule for matching attributes between the two directories; for example, the **department** field in the Exchange directory is automatically mapped to the **department** field in the Active Directory. In some scenarios it is desirable to change this map for a customized solution. For example, you can map the Exchange **Custom-Attribute-3** attribute (called **Extension-Attribute-3** in LDAP) to the Active Directory **employeeID** attribute.

These matching rules are held on the **Default ADC Policy** object for the ADC (not CA-specific) in a field called **msExchServerXSchemaMap**, in which *X* equals 1 for Active Directory-to-Exchange mapping and 2 for Exchange-to-Active Directory mapping.

You can view or change this mapping table by using a tool, such as **Ldp**, in binary mode. The format of the property is very specific and you must make changes carefully.

Appendix: Schema Updates Made by the Exchange 2000 Server ADC

The following schema updates are applied to an Exchange 5.5 site when an Exchange 2000 ADC is installed and configured to write to that site. These updates are also applied to a site when a server is upgraded to Exchange Server 5.5 SP3.

```
dn: cn=Object-GUID,<SchemaContainerDN>
changetype: add
objectclass: Attribute-Schema
Access-Category: 1
Attribute-ID: 1.2.840.113556.1.2.618
Attribute-Syntax: 2.5.5.10
Is-Single-Valued: FALSE
Admin-Display-Name: Object-GUID
description: objectGUID
MAPI-ID: 35949
OM-Syntax: 4
Heuristics: 3
Extended-Chars-Allowed: 0
Search-Flags: 1

dn: cn=Replication-Signature,<SchemaContainerDN>
changetype: add
objectclass: Attribute-Schema
Access-Category: 1
Attribute-ID: 1.2.840.113556.1.2.619
Attribute-Syntax: 2.5.5.10
Is-Single-Valued: TRUE
Admin-Display-Name: Replication-Signature
description: Replication-Signature
MAPI-ID: 35950
OM-Syntax: 4
Heuristics: 3
Extended-Chars-Allowed: 0
Search-Flags: 0

dn: cn=Unmerged-Attributes,<SchemaContainerDN>
changetype: add
objectclass: Attribute-Schema
Access-Category: 1
Attribute-ID: 1.2.840.113556.1.2.620
Attribute-Syntax: 2.5.5.10
Is-Single-Valued: FALSE
Admin-Display-Name: Unmerged-Attributes
description: unmergedAtts
MAPI-ID: 35951
OM-Syntax: 4
Heuristics: 3
Extended-Chars-Allowed: 0
Search-Flags: 0

dn: cn=Top,<SchemaContainerDN>
changetype: modify
add: May-Contain
May-Contain: 1.2.840.113556.1.2.618
May-Contain: 1.2.840.113556.1.2.619
```

```
May-Contain: 1.2.840.113556.1.2.620
-

dn: cn=Object-GUID,<SchemaContainerDN>
changetype: modify
replace: Search-Flags
Search-Flags: 1
-

dn: cn=Schema-Version,<SchemaContainerDN>
changetype: modify
replace: Range-Upper
Range-Upper: 2506
-

dn: cn=ADC-Global-Names,<SchemaContainerDN>
changetype: add
objectclass: Attribute-Schema
Access-Category: 1
Attribute-ID: 1.2.840.113556.1.2.621
Attribute-Syntax: 2.5.5.12
Is-Single-Valued: FALSE
Admin-Display-Name: ADC-Global-Names
description: msExchADCGlobalNames
OM-Syntax: 64
Heuristics: 5
Extended-Chars-Allowed: 0
Search-Flags: 1

dn: cn=Top,<SchemaContainerDN>
changetype: modify
add: May-Contain
May-Contain: 1.2.840.113556.1.2.621
-

dn: cn=Tagged-X509-Cert,<SchemaContainerDN>
changetype: modify
replace: Description
Description: userSMIMECertificate
-

dn: cn=Tagged-X509-Cert,<SchemaContainerDN>
changetype: modify
replace: Heuristics
Heuristics: 19
```